S. HRG. 112–167

CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 12, 2011

Serial No. J–112–16

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
71–412 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON CRIME AND TERRORISM

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

HERB KOHL, Wisconsin	JON KYL, Arizona
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
AMY KLOBUCHAR, Minnesota	LINDSEY GRAHAM, South Carolina
CHRISTOPHER A. COONS, Delaware	

STEPHEN LILLEY, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM

TUESDAY, APRIL 12, 2011

U.S. SENATE,
SUBCOMMITTEE ON CRIME AND TERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 2:38 p.m. in room SD–226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, Chairman of the Subcommittee, presiding.

Present: Senators Whitehouse, Feinstein, Klobuchar, Coons, Blumenthal, Kyl, and Hatch.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Chairman WHITEHOUSE. Good afternoon, everyone. Thank you all for being here. Today's hearing takes on a topic of vital importance: Cyber Security: Responding to the Threat of Cyber Crime and Terrorism.

We live in the most connected and technologically advanced country in the world. Our electrical engineers, computer scientists, and technology companies have changed the way that the world does business, made our daily lives safer and more enjoyable, empowered free speech in repressive states, and brought the world closer together. These remarkable innovations unfortunately also have given criminals, terrorists, and hostile states new opportunities to steal American property, disrupt our way of life, and compromise our National security.

American consumers are now subject to endless swindles achieved by spear phishing e-mails, malware that turns their computers into unwitting bots sending out malicious spam, or the many varieties of identity theft cooked up by cyber crooks to steal hard-working Americans' privacy and money.

Our country's businesses likewise are under assault by foreign agents who seek to steal American intellectual property, a crime that has reportedly led to the loss of over $1 trillion of value to date; and by criminal hackers who seek to empty out corporate accounts or to blackmail companies by threatening to release stolen trade secrets. These crimes hurt companies' bottom lines and they rob us of American jobs, shuttering small businesses by stealing their core intellectual property, making a new product line unprofitable by letting a foreign company reap the benefit of American research and development, or even preventing the next great American company from bringing the next great innovation to market.

Key elements of our Nation's critical infrastructure such as our electrical grid, financial services system, and telecommunications networks have been probed by malicious actors and in some cases compromised, with the possibility that hostile state actors have buried latent attacks that they can trigger when it would hurt us most. Even our Government, civilian, and military networks are under constant and successful attack.

We need to do more to defeat the massive and worsening cyber threat. I am not alone in this belief. The Majority Leader has recognized that the Senate should act on cyber security legislation. The Commerce, Homeland Security, Intelligence, and Armed Services Committees have been hard at work. This Committee, under Chairman Leahy's leadership, has reported data breach legislation and last week held a hearing that has considered reform of the Electronic Communications Privacy Act. And we hope and expect the administration to weigh in shortly with its proposals to improve our Nation's cyber security.

The Senate has important work ahead. It may be hard and complicated work, but I believe that we can accomplish this task in a bipartisan and well-considered fashion. I particularly look forward to working on this vital national issue with the Ranking Member of this Committee, Senator Jon Kyl.

I know that this is a topic of serious interest and prior work for you, Senator Kyl, and I believe we will make a lot of progress together.

I am very happy, for example, to be working with you to improve public awareness of the cyber security threats facing our Nation on a bill that I hope we can file shortly, and to go on to work on legislation to provide a safe space for joint defense by our private industries to take place.

Today's hearing will explore the nature, scale, source, and sophistication of cyber attacks against consumers, Government agencies, and businesses and industries and compare that to the resources that our Government currently brings to bear on these attacks, as well as investigative and prosecutorial successes and limitations. And it will consider the ways in which the private sector is able to collaborate with law enforcement to defend against and respond to cyber attacks.

We are lucky to have two very strong panels of expert witnesses from inside and outside the administration, including a distinguished professor from Brown University in my home State of Rhode Island, which I am happy to note is already at the forefront of the cyber security field. I thank all of the witnesses for being here today.

Before I turn to Senator Kyl, let me flag my serious concern that our prosecutorial and investigative resources are not appropriately scaled to the threat we face. Even in this time of budget cutting, given the enormous stakes, the cyber threat is simply too dangerous to leave underresourced.

Again, I thank the witnesses for being here and now turn to the Ranking Member, Senator Kyl, for his opening statement. Senator Kyl.

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Thank you, Mr. Chairman, not only for holding this hearing today but for the remarks that you just made.

As one former member of the Intelligence Committee to another, I have been deeply impressed by your commitment to cyber security and your command of the associated issues and look forward to what will be the first of many hearings on this subject before this Subcommittee.

I am also pleased to have been able to work with you to draft the forthcoming legislation that you mentioned regarding cyber security awareness. While this bill may be considered chiefly a place holder for things to come, I think it is an important step because of the multitude of topics that it covers, and that multitude speaks to a larger point and problem.

I know of your frustration that Congress has waited for so long to get cyber security legislative proposals from the White House. This delay has complicated the Congress' task of passing comprehensive cyber security legislation. By my count, there are more than seven full committees on the Senate side alone, including the Judiciary Committee, that will be involved in drafting a comprehensive bill. This will take time, and we are long overdue for the President to share his proposals for cyber security legislation so that we can get started.

I am eager to hear from our expert witnesses about how they think Congress should differentiate cyber crime and cyber warfare directed by a state or terrorist group, especially since, I would argue, it does not much matter if a crippling attack on our electric grid, banking system, or other critical infrastructure, or the wholesale theft of billions of dollars of U.S. intellectual property, defense related or purely commercial, is being directed by a cyber mafia or a cyber army. It is the responsibility of this Government to stop the attack either way. If we are just focusing on prosecuting these attacks of cyber crime, then I would say we have failed.

So I look forward to the testimony of our witnesses, Mr. Chairman, and I hope there will be stimulating and informative rounds of questions thereafter. Thank you.

Chairman WHITEHOUSE. Thank you, Senator Kyl.

If I could ask the witnesses to stand for the oath. Do you affirm that the testimony you are about to give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. WEINSTEIN. I do.

Mr. SNOW. I do.

Mr. MARTINEZ. I do.

Chairman WHITEHOUSE. Thank you very much. Please be seated.

We will just go right across the table with the witnesses, beginning with Jason Weinstein. Jason Weinstein currently serves as Deputy Assistant Attorney General in the Department of Justice's Criminal Division where he oversees the Division's efforts to combat computer crime and intellectual property crime, as well as antigang and violent crime efforts and human rights and human-smuggling programs.

Before joining the Criminal Division, Mr. Weinstein served as chief of the Violent Crimes Section of the U.S. Attorney's Office in Baltimore and before that as an Assistant United States Attorney in the U.S. Attorney's Office for the Southern District—the Sovereign District—of New York. We are delighted that he is here, and your full statement will be a matter of record, so if you could please make whatever statement you would like to make orally within the allotted time, I would appreciate that.

STATEMENT OF JASON WEINSTEIN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. WEINSTEIN. Thank you, Mr. Chairman. The Sovereign District of New York jokes got a lot funnier after I moved to Baltimore.

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and other members of the Subcommittee, and I thank you for the opportunity to appear before you today.

As we all know, the explosive growth of the Internet and other modern forms of communication has revolutionized nearly every aspect of our daily lives. But at the same time, it has also revolutionized crime, and increasingly the Internet has being exploited by criminals throughout the world to commit a staggering array of crimes.

From around the corner or around the globe, skilled hackers work every single day, and many times every day, to access the computer systems of Government agencies, of universities, banks, merchants, and credit card companies to steal large volumes of personal information and to perpetrate large-scale data breaches that leave tens of millions of Americans at risk of identity theft.

Our information infrastructure is under constant attack from these criminals as well as from terrorists and nation states that seek to exploit our dependency on information technology to threaten both our economic and our National security.

So for these reasons, now more than ever cyber security has to be a national priority. This administration is committed to implementing a comprehensive framework that will allow us to bring all appropriate tools, criminal and otherwise, to bear against cyber criminals, terrorists, and other malicious actors. And the Department of Justice plays a critical role in that effort.

The Justice Department works closely with our partners throughout the Government to support the Nation's efforts to support cyberspace, including by providing legal support and helping to ensure that we vigorously protect privacy and civil liberties. The Department also plays a leading role in counterintelligence and national security investigations that uncover threats to our computer networks from terrorists and state actors.

But perhaps one of the Department's most important contributions to the Nation's overall cyber security is the investigation and prosecution of cyber criminals as we seek to incapacitate and punish the cyber criminals of today and to deter the cyber criminals of tomorrow. And in that important work, our prosecutors from the Criminal Division, from the National Security Division, and from the U.S. Attorney's Offices enjoy very strong relationships with our

law enforcement agency partners, and in particular with the other two agencies represented on the panel with me today—the FBI and the Secret Service.

Those strong relationships and the dedication and skill of our prosecutors and our agents have led to a number of major enforcement successes, including the following:

In August of 2008, the Department, working with the Secret Service, announced one of the largest hacking and identity theft cases ever prosecuted, in which charges were brought by the U.S. Attorney's Offices in three different districts—Massachusetts, Southern California, and Eastern New York—against 11 members of an international ring responsible for the theft and sale of more than 40 million credit and debit card numbers that had been stolen from major retailers.

The defendants were from all over the world—from the U.S., from Estonia, Ukraine, China, and Belarus—and they included one of the world's top hackers, Albert Gonzalez. Gonzalez pled guilty to the charges and was sentenced to 20 years in prison, which is one of the longest sentences ever imposed in a hacking case.

In November 2009, following a year-long investigation led by the FBI, the Department announced the indictment in the Northern District of Georgia of a hacking ring responsible for executing a global fraud scheme involving defendants from Estonia, Russia, and Moldova. The defendants were charged with hacking into a network operated by the credit card processing company RBS WorldPay, compromising its data encryption and then providing a network of cashers throughout the world with counterfeit payroll debit cards. Those cashers used those cards to withdraw over $9 million from more than 2,100 ATM machines in at least 280 cities worldwide, and they conducted that coordinated global cashing operation in less than 12 hours.

Those cases as well as the others referred to in my written testimony illustrate the scope of the Department's efforts to pursue cyber criminals. But, significantly, they also reveal the global nature and the global reach that cyber criminals can have.

The criminals responsible for those and other large-scale intrusions often live in and operate from foreign jurisdictions. It is often literally impossible to identify, arrest, and prosecute the offenders or to obtain critical evidence that we need to prosecute the offenders without the assistance of foreign law enforcement. And for that reason, our work does not stop at our shores.

Due to the transnational nature of most cyber security incidents, continued close coordination and cooperation with our foreign partners is critical to our success. And in that connection, we rely on the International Convention on Cyber Crime to provide a framework for efficient cooperation among nations involving electronic crime.

The Department is proud of these cases and all of our cyber security efforts, but there should be no doubt, as the Chairman and the Ranking Member said, that the cyber threats to our Nation are growing and evolving, and we must remain vigilant and prepared to confront them, and we will continue to work with our Government and private sector partners and the Congress to meet that challenge.

Thank you for the opportunity to be here today to discuss this issue with you, and I would be pleased to answer your questions.

[The prepared statement of Mr. Weinstein appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much. We are delighted to have you with us.

We will go on next to Gordon Snow, who is the Assistant Director of the Cyber Division at the Federal Bureau of Investigation. He was named section chief of the Bureau's Cyber Division on January 2008 and now leads the Division's Cyber National Security Section and the National Cyber Investigative Joint Task Force. From January 2008 to January 2009, he was detailed to the Director of National Intelligence on the National Counterintelligence Executive. During that assignment, he led the effort in drafting the goverment-wide Cyber Counterintelligence Plan under the Comprehensive National Cyber Initiative.

Prior to that, Mr. Snow's work with the FBI took him to Afghanistan as the FBI's on-scene commander for the Counterterrorism Division, to Silicon Valley working on the High Value Computer Crimes Task Force, and to Yemen and East Africa.

Thank you, Mr. Snow. Glad to have you with us.

STATEMENT OF GORDON M. SNOW, ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. SNOW. Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and members of the Subcommittee. I am pleased to appear before you today to discuss the cyber threats facing our Nation and how the FBI and our partners are working together to respond to the threat of cyber crime and terrorism.

As the Committee is aware, cyber attacks have increased over the past 5 years and are expected to grow. We have reached the point that, given enough time and motivation and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet. The FBI has identified the most significant cyber threats to our Nation as those with high intent and high capability to inflict damage or death in the U.S., to illegally obtain sensitive or classified information, or to illicitly acquire assets.

I would like to focus my remarks today on a few of the many threats facing the private sector, including threats against infrastructure, intellectual property, individual businesses, and our partnerships to address these threats.

U.S. critical infrastructure faces a growing cyber threat due to the advancements in the availability and sophistication of malicious software tools. The recent security breach by unauthorized intruders into the parent company of NASDAQ is an example of the kind of breaches directed against important financial infrastructure.

Industrial control systems, which operate the physical processes of the Nation's pipelines, railroads, and other critical infrastructures, are at great risk of cyber exploitation.

Similarly, new "smart grid" and "smart home" products could also be exploited by cyber criminals, nation states, and terrorists.

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00010 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

These systems need to be developed and implemented in ways that will provide protection from unauthorized use.

Intellectual property rights violations, including theft of trade secrets, digital piracy, and trafficking in counterfeit goods, also represent high cyber criminal threats, resulting in losses of billions of dollars in profits annually. These threats pose significant risk to U.S. public health and safety via counterfeit pharmaceuticals, electrical components, aircraft parts, and automobile parts.

Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime.

One facet of this are botnets, or networks of compromised computers controlled remotely by an attacker. Criminals use botnets to facilitate online schemes that steal funds or data, to anonymize online activities, and to deny access by others to online resources. The botnets run by criminals could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure.

The potential economic consequences are severe. Often businesses are unable to recover their losses, and it may be impossible to estimate the damage. Many companies prefer not to disclose that their systems have been compromised, making it impossible to accurately quantify. Consequently, these damages estimates have ranged from millions to hundreds of billions.

Thanks to Congress and the administration, the FBI is devoting significant resources to this threat. Our partnerships with industry, academia, and across all of government have led to a dramatic improvement in our ability to combat this threat.

The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation states, and terrorists.

The FBI has cyber squads in each of its 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners.

However, the FBI cannot combat the threat alone. Through the FBI-led National Cyber Investigative Joint Task Force, we coordinate our efforts with over a dozen Federal partners throughout the intelligence community and the Department of Defense. We also partner through NCIJTF with other Federal law enforcement agencies to include most prominently the United States Secret Service. The FBI has also embedded cyber staff in other intelligence community agencies through joint duty and detailee assignments.

In addition to our 61 legal attaches overseas, we currently have FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations. These cyber agents have identified organized crime groups, supported FBI investigations, and trained foreign law enforcement officers for more than 40 nations.

InfraGard is a prime example of the success of public-private partnerships. Under this initiative, private industry leaders work with the FBI to ward off attacks against critical infrastructure. Over the last 15 years, this initiative has grown from a single

chapter to more than 86 chapters in 56 field offices with 42,000 members.

In addition to InfraGard, the FBI partners with the National White Collar Crime Center and the Internet Crime Complaint Center and the National Cyber Forensic and Training Alliance. We also partner with the information-sharing and analysis centers through the Department of Homeland Security and the National Center for Missing and Exploited Children.

Chairman Whitehouse, Ranking Member Kyl, and members of the Subcommittee, in the interest of time today, I have touched upon a few of the more significant cyber threats facing our Nation. I appreciate the opportunity to come before you and share the work the FBI and our partners in the community are doing to address the cyber threat in this country and am happy to answer any questions you may have.

[The prepared statement of Mr. Snow appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Assistant Director Snow.

Our next witness, Pablo Martinez, is Deputy Special Agent in Charge of the Criminal Investigation Division, Cyber Crime Operations, at the United States Secret Service. In this capacity, he develops and implements policy for all cyber investigations conducted by the Secret Service. Mr. Martinez began his career at the Service in 1991, and in 1999 was transferred to the Presidential Protective Division. In 2003, Mr. Martinez was promoted to the supervisory ranks of the Criminal Investigative Division, where he was tasked with expanding the Service's Electronic Crimes Task Force. During that time, he oversaw the first major cyber operation conducted by the Secret Service, Operation Firewall, in which over 30 online criminals were apprehended worldwide in a simultaneous roundup.

Glad to have you with us, Agent Martinez.

STATEMENT OF PABLO A. MARTINEZ, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATION DIVISION, U.S. SECRET SERVICE

Mr. MARTINEZ. Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the role of the Secret Service in cyber investigations.

On February 1, 2010, the Department of Homeland Security delivered the Quadrennial Homeland Security Review, which established a framework for homeland security missions and goals. I would like to share just a few sentences from the QHSR because it underscores the need for a safe and secure cyberspace:

"As we migrate more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. We face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services."

In order to maintain a safe and secure cyberspace, we have to disrupt the criminal organizations and other malicious actors engaged in high consequence or wide-scale cyber crime.

To address the threats posed by these transnational cyber criminals, the Secret Service has adopted a multi-faceted approach to investigate these crimes while working to prevent future attacks. A central component of our approach is the training provided through our Electronic Crimes Special Agent Program, which gives our special agents the tools they need to conduct computer forensic examinations on electronic evidence obtained from computers, personal data assistants, and other electronic devices. To date, more than 1,400 special agents are ECSAP trained. In fact, the Secret Service values this training so highly that the basic level is now incorporated as a part of the curriculum that all special agent trainees receive at our James J. Rowley Training Center.

In addition, since 2008, the Secret Service has provided similar training to 932 State and local law enforcement officials, prosecutors, and judges, through the National Computer Forensics Institute, located in Hoover, Alabama. The Secret Service's commitment to sharing information and best practices with our partners, the private sector, and academia is perhaps best reflected through the work of our 31 Electronic Crime Task Forces, including two located overseas in Rome, Italy, and London, England.

To coordinate these complex investigations at the headquarters level, the Secret Service has enhanced our cyber intelligence section to identify transnational cyber criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. In the past 2 years, CIS has directly contributed to the arrest of 41 transnational cyber criminals who were responsible for the largest network intrusion cases ever prosecuted in the United States. These intrusions resulted in the theft of hundreds of millions of credit card numbers and the financial loss of approximately $600 million to financial and retail institutions.

As an example, the partnerships developed through our ECTFs, the support provided by our CIS, the liaison established by our overseas offices, and the training provided to our special agents via ECSAP were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems. The August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a collection device to capture payment transaction data.

Our investigation revealed data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group. Furthermore, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data.

As a result of our investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to 20 years in Federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working

with its law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

Chairman Whitehouse, Ranking Member Kyl, and distinguished members of the Subcommittee, the Secret Service is committed to our mission of safeguarding the Nation's cyber infrastructure and will continue to aggressively investigate cyber and computer-related crimes to protect American consumers and institutions from harm.

This concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service.

[The prepared statement of Mr. Martinez appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Agent Martinez. I appreciate having you here.

One of the purposes of this hearing is to look into the comparison between the size of the threat and the resource that is dedicated to it, and if I may, Mr. Weinstein, let me ask—I have some numbers here about Criminal Division deployment at the Department of Justice. And just by way of comparison, we have looked at OCDETF, the Organized Crime Drug Enforcement Task Force program; we have looked at the Organized Crime Task Force, dedicated to traditional Mafia organized crime; and we have looked at the cyber staff. And the numbers that I have are that there are just under 90 attorneys in the Criminal Division dedicated to traditional organized crime. There are 13 attorneys in the Criminal Division dedicated to the OCDETF program, but the OCDETF program is very much a field-based program, and so they are sort of the local touch point for over 1,000 staff out in the field, including more than 550 attorneys out in the field. So it is a pretty robust field program behind those 13 attorneys at Main Justice.

In the context of that range, we have been told that there are 40 attorneys in the Criminal Division who are dedicated to computer intrusions and other hacking cases. There are additional attorneys who are dedicated to child exploitation, to appellate cases, to other crimes that may have a computer component but are not the direct hacking cases.

It strikes me that if the numbers are correct that there is as much as $1 trillion, I contend that we are on the losing end of the biggest transfer of wealth in the history of humankind through theft and piracy in this country right now, that it is being done through cyber crime, and that it is a very, very significant national security and economic challenge.

Senator Feinstein and Senator Kyl and I all have also served on the Intelligence Committee, and while much of what we know from that Committee is classified, in the public hearing the Director of National Intelligence Jim Clapper listed the national security threats that he felt he was obliged to address as the new DNI, and he put cyber security No. 1 above everything else.

And so that was kind of noteworthy, and in that context it strikes me that having fewer attorneys dedicated to computer intrusions at Main Justice than are dedicated to old-fashioned, traditional organized crime is a sign that we here in Congress need to provide you with more resources to focus on the cyber threat.

What is your sense of that?

Mr. WEINSTEIN. Let me, before I answer your question, put those numbers in a little bit of context.

You are right in observing that the OCDETF program is mostly a field-based program, so it is not unexpected that that is a relatively low number dedicated to that.

The organized crime number which you quoted, which is about 89 attorneys, actually it was organized crime broadly defined. That is to say, it is traditional organized crime like LCN, Mafia-type cases; it is gang cases; it is drug-related organized crime like drug cartel cases, which are pursued as enterprises; and it includes international organized crime. And in that sense, especially with international organized crime, there is some overlap with our cyber security and cyber crime efforts.

I actually also, along with another Deputy AG, oversee the organized crime program, and increasingly the priority of our international organized crime program is to go after transnational crime groups that involve cyber threats. So there is some overlap.

The other thing I would add is that the 40 attorneys that you quoted that are cyber specific, those are the attorneys who are in the Computer Crime and IP Section, which I have had the honor to supervise. There are a substantial number of other attorneys, like in the Fraud Section, who also in the course of their fraud work focus on fraud cases that have a cyber component.

Having said all that, it is really undeniable that the scope of the problem, which is growing every day, far outpaces the resources that are available to pursue it currently. And so I think that this is the kind of problem that takes a dedicated stream of resources, but it also takes dedicated training and expertise so we can keep pace with the methods that our cyber actors are using.

I would add that in the President's 2011 budget, which I think now is a collector's item, there was a request for four additional cyber attorneys. In the 2012, there is actually a request for six, and those six attorneys are CHIP prosecutors, computer hacking and IP prosecutors. But for the first time, they will be CHIP prosecutors who are placed overseas, I think to reflect the recognition that fighting this problem requires going beyond our borders to do it.

The President's proposal, the President's budget proposal, would put six of these CHIPs, who we would call ICHIPs, international CHIPs, in regions throughout the world that have a high concentration of cyber crime and IP theft activity so that they can not only help American prosecutors at home on their cases but also help those contractors beef up their own capacity to pursue cyber criminals in their own borders.

Chairman WHITEHOUSE. My time has expired, but let me ask just one more question before I turn to Senator Kyl because there is also field staff, attorneys out in the U.S. Attorneys' Offices, who are dedicated to this. But it is my understanding that the—if you could confirm this, it is my understanding that the AUSAs who are your cyber designees are obliged to participate in conferences on cyber, be a point of contact for the office on cyber; if there are conference calls, they are the person for the office who would participate, but they need not direct their prosecutive attention to cyber cases. They are to be deployed as the U.S. Attorney and the first assistant and the head of the Criminal Division see fit, and in that

sense it is something of an overcount to describe them as full-time—it would be something of an overcount to describe them as full-time cyber prosecutors, would it not?

Mr. WEINSTEIN. I think, Senator, it depends on where—Mr. Chairman, it depends on where they are. In some districts, especially districts with very active FBI or Secret Service cyber squads in them, and with a heavy concentration of these cases, the CHIP prosecutors work exclusively on those cases.

Chairman WHITEHOUSE. But in some they may not——

Mr. WEINSTEIN. Some districts they may not. And the role really has three or four aspects to it. One is to work on this case——

Chairman WHITEHOUSE. Well, since I am over my time——

Mr. WEINSTEIN. OK.

Chairman WHITEHOUSE [continuing]. And since I have my Ranking Member waiting, let me—we can pursue that in the——

Mr. WEINSTEIN. OK.

Chairman WHITEHOUSE [continuing]. Later discussion.

Senator Kyl.

Senator KYL. Well, thank you, Mr. Chairman. These are all right-on questions, and in a related area, it is not only resources but also authority.

Agent Martinez, I would like to ask you a question about comments you made in your testimony in which you referred to going dark, the going-dark problem, whereby there is a gap between the legal authority that you have to intercept electronic communications and the provider's practical ability to intercept those communications. And you quoted and endorsed the statement by the FBI Chief Counsel, who had testified in the House of Representatives, that there is—excuse me. She said, "There are significant law enforcement challenges in light of the pace of technological advancements."

Are there specific tools that you think Congress could provide you and your counterparts in domestic law enforcement and intelligence to better mitigate this problem? Can you share them with us today? If not, could I ask all three of you really to provide to this Committee your proposals for improving the authorities that all of you need to tackle the problems that you have identified here today?

Mr. MARTINEZ. Yes, Senator Kyl, we did endorse Chief Counsel's statements on that. We believe that cyber criminals are at the tip of the spear when it comes to exploiting technology. The types of communications that cyber criminals use or have been using for many years are now just starting to come into the forefront of crimes being committed by traditional criminals. So cyber criminals have been using instant message, have been using VOIP systems, have been communicating via the computer for many, many years, and we believe as technology continues to develop you are going to continue to see cyber criminals exploiting that capability because they seem to have the most knowledge when it comes to utilizing devices like that.

I believe right now there are several working groups that have been established, you know, at the request of the administration, both at the legislative level and at the technical working group level. The Secret Service participates in a technical working group

being led by the FBI, and we are in the process right now of finalizing some of our recommendations that I believe the administration is looking to put forward.

Senator KYL. Great. We will appreciate that, hearing from FBI, Justice Department, and Secret Service, whomever, to assist us in giving you the authority you need.

Assistant Director Snow, I would like to ask you, could you explain the FBI's role in the so-called Team Telecom? And then I've got a couple specific questions about what I understand that team is engaged in, the advisory role to the Federal Communications Commission by the FBI. Is that not a term you are familiar with?

Mr. SNOW. Sir, I apologize. It is not a term I am familiar with. It usually runs out of our Operational Technology Division, which would, along with our Office of General Counsel——

Senator KYL. OK. Well, let me just ask you to generally describe concerns that you all have about telecommunications computers that have links to foreign governments or foreign militaries providing telecommunications equipment, software, network management services and the like here in the United States.

Mr. SNOW. Sir, I guess the best way to answer that is in another forum we could probably go more in-depth, and I would be more than willing to provide you the personnel and myself and availability to address those questions.

Senator KYL. Well, is it fair to say that there is a significant concern about this and that you do play a role, that the FBI does play a role along with other intelligence services in advising our Government departments with respect to these threats?

Mr. SNOW. Yes, sir, absolutely. Always a concern from any facet, a country adversary that comes in and that would either manipulate or use our supply chain to our disadvantage. So if so many things in the supply chain, whether it is a counterfeit part, a counterfeit CHIP, something that could be implanted, an executable piece of malware, a piece of additional code that would be in our telecom system.

Senator KYL. When you review the offer of such a company to open themselves up to third-party or independent review to deal with those supply chain kinds of problems, is it possible for you to go through millions of lines of software code to make 100 percent certain that there is not anything malicious built in that is capable of being activated at a moment of a cyber criminal's or cyber warrior's choosing?

Mr. SNOW. I do not think, sir, that we have that capability right now in the U.S. Government to go through millions of lines of code. It is very work intensive. I think we know that code now is cobbled together from many pieces. I think sometimes even the programmers and people that design that code are not even sure what is in that code. They will use other pieces, freely available pieces on the outside to assemble that program. And we do provide under the CFIUS process counsel, guidance, direction, and information to the decisionmakers across the Government in order to make those decisions, along with the Department of Justice that runs the CFIUS program.

Senator KYL. I appreciate it. Thank you.

Chairman WHITEHOUSE. Senator Coons.

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00017 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

Senator COONS. Thank you, Senator, and thank you to both Senator Whitehouse and Senator Kyl for convening this hearing today, and to our panel.

You have all testified to the different ways in which your respective agencies are working together with State and local law enforcement, and to some extent, the private sector, the intelligence agencies, and our armed forces to combat cyber crimes, and I am just interested initially in your opinion whether States and local law enforcement have the right resources, have the right training, have the right capabilities to buildup their investigative capabilities as well as their defensive capabilities.

You made reference, Agent Martinez, in your testimony to the National Computer Forensics Institute and where the 900 folks have been trained. I think that is a great start. There was also a reference, I think by Mr. Snow, to 42,000 members of the FBI's InfraGard.

If you could, in order to speak to the training standards we are trying to hit, the resources State and local law enforcement and Government have, and what additional resources do we need in order to be able to develop a nationwide professional cadre of folks in law enforcement, in the intelligence community, and, frankly, in the private sector? Please.

Mr. MARTINEZ. Thank you, Senator. From our perspective in law enforcement, what we have basically done is taken our ECSAP model—that is a three-tier model, BICEP, NITRO, and computer forensics—and we have mirrored that curriculum at the National Computer Forensics Institute where we not only teach law enforcement but also prosecutors and judges. We are firm believers that you not only have to train the agents or the law enforcement officers, but you have to make sure that they can explain or they can articulate in a layman's term the case to a prosecutor who can then also explain the facts in layman fashion to a judge who you are going to have to get the warrants signed to. So that is why it has been—it is important for us to train all three aspects.

So far, like I stated in my statement, we are over 900. We are looking to try to expand the amount of law enforcement personnel that we train. What we try to focus on, since we have the 31 Electronic Crime Task Forces, we try to focus on individuals who are members not only of our task force, but potentially a State and local cyber task force or an FBI task force because they are in the most need of having this specialized training. We believe that by doing that we are multiplying our resources, and we can force multiply and work investigations not only at the Federal level but at the State and local level.

And like I said, we continue to work with these partners at the State and local level to try to get them a better understanding of some of the issues with cyber crime and some of the ways to tackle the problem.

Senator COONS. Mr. Snow.

Mr. SNOW. Sir, as Mr. Martinez talked about, the good news portion of the story is that we are making progress on trying to help assist and train those personnel. I think inwardly, though, if we are more reflective, it is a difficult task to make sure that all our personnel are trained, not only that they are trained but what is

the process that we used in order to make sure that we keep them current and how we retain those personnel.

So I would not want to classify all State and local law enforcement officers as being in the position we were in about 10 years ago. We talked recently about the going-dark issue, and we also talk about how difficult it is to bring those people up to speed. But I would say—because I know we have very talented individuals from State and local entities that are in our regional computer forensic labs that are run nationally across the country.

However, many of those departments and agencies, you know, hundreds of thousands of sworn law enforcement officers across the country, have a difficult time coming up with that money, that training, the availability of their personnel as they try just to meet hiring and payrolls.

Senator COONS. And if I could, just a follow-on question to the Deputy Assistant Attorney General, Mr. Weinstein. One of the areas I am most concerned about is intellectual property theft, particularly trade secrets. American companies are some of the most innovative in the world. In your written testimony, there was an example of a successful theft from Dow Chemical that had significant long-term consequences for them.

Where are we in terms of providing coordination, resources, and standards for training that will help the private sector understand how to defend against these threats and then the prosecutorial resources to, as you put it, once these better locks are broken, actually then capture the CMS who have broken them?

Mr. WEINSTEIN. Well, Senator, perhaps in IP crime, unlike any other type of crime, we rely heavily on the victim companies to report the crimes to us and to be able to recognize them when they occur, then to provide us with access to the information we need to successfully investigate and prosecute them.

One of the things that CCIPS does in conjunction with the CHIP prosecutors throughout the country is conduct extensive outreach with potential victim companies in various regions. In the Pacific Northwest it might be Microsoft, or computer companies in Delaware and other States, it may be, you know, companies that are the significant industries in those States. And what we try to do is explain to them where the risks are, how to recognize when there is a potential trade secret theft or other IP crime, and then how to make a referral to us, either to us directly or to the FBI or to the IPR Rights Center, which is jointly operated by ICE and by the FBI.

So we do that nationally, and we do that regionally. We go region by region throughout the country to try to make sure that companies that are at the greatest risk are aware of what is going on out there and how to protect themselves from it; and then if they are violated, how to report it to us so we can pursue it.

Senator COONS. Thank you.

Chairman WHITEHOUSE. Senator Hatch.

Senator HATCH. Well, thank you, Mr. Chairman, Chairman Whitehouse. I thank you and applaud you for your efforts in this area.

The distinguished witnesses represent a balance of all those affected by cyber criminal and terrorism—Government, the private

sector, and, of course, academia. For successful cyber security policy, we must encourage partnerships among many sectors. This cannot be solely a Government-led initiative.

Now, Mr. Snow, China is directing the single largest, most intensive foreign intelligence gathering effort since the cold war against the United States. Methods for conducting informational warfare to advance the goals of a nation state might also involve secretly sponsoring terrorists.

Now, China is often cited as providing Government support to computer hackers, and as Richard Clarke, a former White House adviser for infrastructure protection and counterterrorism, discusses in his book, "Cyber War," the Chinese military has placed a new emphasis on information warfare methods. Specifically, they have proposed to attack enemy financial markets, civilian electricity networks, and telecommunication networks by way of computer viruses and, of course, hacker detachments.

Now, it remains very difficult to determine the true identity, purpose, or sponsor of a cyber attacker. Can you tell me, does the FBI have sufficient capability to identify an attack that is state sponsored versus a criminal enterprise?

Mr. SNOW. Senator, obviously, once again, in a different forum we can go more in-depth to your question, but let me answer it in a form that I can today.

Senator HATCH. Sure.

Mr. SNOW. Through the National Cyber Investigative Joint Task Force, which I mentioned in my opening statement, we have 18 intelligence community agencies and others there. We use a concept that is called the threat focus cell concept where we bring all individuals from the community that would address a threat. The successes that we have had have been many. The problem with it is that there are still some very high profile cases that we have seen just by looking through the Wall Street Journal and any other media outlet we have out there where we still do not know to this day who the attacker is, what state we can attribute it to, or who that person behind the keyboard was, who that human person was that actually controlled that attack or directed that attack.

Senator HATCH. Mr. Martinez, several months ago, as Chairman of the Senate Republican High-Tech Task Force, I requested that the Secret Service provide an extensive briefing on transnational organized crime and international cyber investigations. I thought that briefing was pretty helpful. Now, while that briefing was not classified, it certainly was law enforcement sensitive and provided the task force members a fantastic overview of the transnational crime groups, primarily located in Russia and Eastern Europe.

During that briefing Secret Service officials profiled a particular hacker known as "BadB," who was an accomplished hacker in Russian cyber crime circles. Fortunately, he was arrested overseas based on the investigative work of the Secret Service.

Now, I want to take this opportunity to applaud you and the Secret Service for its work in that case and others, including the Nation's largest identity theft case that occurred at TJX and Heartland Systems. That case had an extensive international cyber crime connection.

Now, No. 1, what presence does the Secret Service have overseas in countries such as China and Russia? And, No. 2, what other mechanisms does the Secret Service have in place to identify countries with the potential for cyber crime?

Mr. MARTINEZ. Thank you, Senator Hatch. Yes, the Secret Service has, I believe—and it is in my written statement. I believe it is 22 overseas offices. And in countries where we do not have an office, we take a regional approach where we have agents that are specifically assigned to those countries. We do have an office in Russia, and I am glad to announce that 2 weeks ago we got our long-term visa to open up our office in Beijing, so we are very happy about that.

In addition to that, though, we rely a lot on our foreign law enforcement partners, and as I stated earlier, we have two foreign electronic crime task forces. So what we have done is we have taken the concept of the domestic Electronic Crime Task Force that Congress enacted back in 2002, and we have used that same approach to our overseas offices. In doing so, we collaborate a lot with our foreign law enforcement partners. Just like the FBI does, we have agents embedded into cyber crime units, and specifically agencies in specific hot spots around the world.

We believe it has been very successful, and we have capitalized on the relationships and partnerships with these law enforcement organizations in order to apprehend some of these high-value targets.

But in addition to that, one of the things we have recently done, as we did last year, we did what is called the Verizon/Secret Service 2010 Data Breach Investigative Report, where we take information for our investigations and we publish that out to the private sector. Well, the 2011 study that is about to come out in 2 months not only includes data from Secret Service and Verizon investigations, but it also includes information from the National High-Tech Crimes Unit in Holland.

So, once again, there we are leveraging the resources and the abilities of our foreign law enforcement partners, and the lessons learned, the best practices, and the information that we have obtained through our criminal investigations, we are pushing that out to the private sector through things such as the DBI Report.

Senator HATCH. Mr. Chairman, could I just make a short set of remarks?

Chairman WHITEHOUSE. Of course, Senator.

Senator HATCH. Thank you very much, both of you. I did not have time to ask you any questions, Mr. Weinstein, but I appreciate the work you are doing.

There is no doubt that we need to have a coordinated effort between Government and the private sector to address cyber crime abroad, and that is why last Congress I introduced, with my colleague Senator Gillibrand, an international cyber crime bill.

Now, our common-sense approach was widely supported amongst those who are affected by these crimes on a daily basis. In the coming weeks we plan to introduce this bill which will improve and strengthen the Government's response to international cyber crime. I would like you to look at that and tell us where we can make it better and what your suggestions are for us so that, when we intro-

duce it, it will be truly something that will be bipartisan and everybody can support.

Thank you, Mr. Chairman. I appreciate it.

Chairman WHITEHOUSE. Of course, Senator.

Our next questioner is not only a distinguished member of this Committee but also the Chairman of the Intelligence Committee. Senator Feinstein.

Senator FEINSTEIN. Thank you very much. I want to thank you, Senator Whitehouse for your work in this area. As Chair of Intel, I asked you to head a cyber task force, along with Senator Mikulski and Senator Snowe, and I want everybody to know that the three of you did a wonderful job, and our information is much fuller and richer because of it. So thank you for the work.

One of the things that apparently you accomplished was the declassification of a lot of material of some of the robberies that had taken place going back to 2008 that we on Intel knew about—excuse me, I have a cold—but could not talk about. And on January 3rd of this year, the Director of National Intelligence wrote you a letter essentially saying that we have compiled unclassified and in some cases declassified material designed to explain the variety of cyber threats and to provide real-world examples of damage in nontechnical terms.

This was provided to the Congress and other elements of the executive branch. I want to go over some of it which has now been declassified.

In 2008, the Royal Bank of Scotland lost almost $10 million withdrawn from ATMs in 49 cities worldwide.

Citibank, a cyber theft scheme resulted in over $10 million in losses. Now, that is according to news reports.

Nationwide retailer T.J. Maxx, 45 million credit and debit cards stolen in 2007.

Heartland Payment Systems, tens of millions of credit card numbers compromised in 2009. And it goes on and on and on.

Mr. Snow, I believe in your testimony you indicated that in 2010 you arrested 202 individuals for criminal intrusions, up from 159 in 2009, and obtained a record level of financial judgments for cases amounting to $115 million compared to $85 million in 2009.

Now, we have looked at some of this and seen a lot of attacks coming from Russia, from criminal elements in Russia, from China, and from other countries, but I think those were the two big ones.

I would like to ask this question: Where do you see the majority of major attacks emanating from? And what is being done to stop this?

Mr. SNOW. Senator, right now we see on the criminal side a majority of attacks coming from the individuals that are located in Russia, obviously different from the Russian state, and Eastern European countries. We see a very strong network of a cyber underground, very closely associated with almost an eBay or an Amazon type system where, you know, once you receive a service from one of these cyber criminals, which are able to just combine together in chat rooms in this cyber underground, which are allowed to buy different pieces that they need to carry out the attack, to execute the attack, to have the cashers, the mules to receive the funds from the attack. They are all graded and rated.

So we see that very large part of the world that is extremely connected being an area where a lot of the threat is coming from on the criminal side right now.

Senator FEINSTEIN. How many arrests have been made? And how do they get made? And how do individuals get prosecuted?

Mr. SNOW. They get prosecuted—and I will refer back to DOJ after I finish my statement, but they get prosecuted in different realms. Some countries, depending on what the MLAT or the extradition treaty is, will either agree to extradite an individual if we have provided the information for them. As Mr. Martinez talked about, with the collaboration that we are working with these other countries, some will abide by the extradition treaties that we have and bring the people back here to the United States.

Senator FEINSTEIN. Are the Russians cooperative in that regard?

Mr. SNOW. We have not had the Russians—they have been cooperative in the joint prosecution arena.

Senator FEINSTEIN. Have any Russian Mafia people been arrested and prosecuted?

Mr. SNOW. I would defer the Mafia side, but are you talking cyber organized crime?

Senator FEINSTEIN. Yes.

Mr. SNOW. Yes, ma'am.

Senator FEINSTEIN. And has Russia cooperated with the United States in going after them?

Mr. SNOW. Russia has helped in large part in many of the cases that we have been involved in. We have exchanged information with the Russian individuals that work cyber crime, and we are still working on those types of relationships with them.

Senator FEINSTEIN. Thank you very much. Thank you. I am glad to hear that.

Thanks, Mr. Chairman.

Chairman WHITEHOUSE. Thank you, Chairman Feinstein.

Next is Senator Klobuchar, then Senator Blumenthal.

Senator KLOBUCHAR. Well, thank you very much, Chairman Whitehouse, for holding this hearing, and I truly believe that protecting our Nation's cyber infrastructure is critical as we increasingly depend on it for everything from paying our utility bills to our financial services.

The innovation surrounding a free and transparent Internet has been great for our economy, but we have also opened ourselves up to risks, and those are risks that, unfortunately, criminals try to exploit.

I am working with Senator Hatch on a cloud computing bill, and we hope to introduce it soon. And I really do see that cloud computing has the potential to alleviate some of the concerns in the cyber security field, particularly by introducing economies of scale and making sophisticated protection available to all users on the cloud. However, it also raises some unique diplomatic issues because data is being stored in multiple countries.

Could you talk, maybe Mr. Weinstein, about issues of international jurisdiction faced by your agencies when investigating cyber crime or, Deputy Director Snow, involving cloud computing? And would better international agreements be helpful to enforce the rules?

Mr. WEINSTEIN. We flipped and I won.

Senator KLOBUCHAR. I noticed that, yes.

Mr. WEINSTEIN. Senator, I cannot speak specifically to international issues involving cloud computing. It is a relatively new phenomenon, at least known by that name. But I can say that, as a general matter, it is increasingly important that we have strong agreements, international agreements, either multilateral or bilateral agreements, with our foreign law enforcement partners because so often the targets or the instrumentalities of the crime are located overseas, even if the data is not overseas.

For example, in the cases that Senator Feinstein just mentioned, in the TJX intrusion, the servers that the data was stored on, the primary hacker was located in Florida. But the data was stored in Latvia and Ukraine.

Senator KLOBUCHAR. Right.

Mr. WEINSTEIN. In the Heartland case that Senator Feinstein mentioned, some of the servers were—there were three servers in the United States, or in three States of the United States; but servers were also in Latvia, Ukraine, and the Netherlands. In the RBS case, some of the targets and evidence was in eight different countries.

What makes the RBS case useful, I think, as an example, though, is that the intrusion was reported to us by the victim company in December of 2008, and the indictment was brought in November 2009. So in less than 11 months, the FBI, working very closely with foreign law enforcement, managed to get the evidence we needed, even though it was across our borders, identify the targets, put fingers at the keyboard, and actually bring charges. And, in fact, BadB, the hacker that Senator Hatch made reference to, is now indicted in that case and is pending extradition.

So when we have got those agreements in place and when the foreign country we are working with has the will, the capacity and the will—because you have got to have both—we can be very effective. Too often the countries have the will but not the capacity, and that we can deal with because we can devote resources, as we do, to training them and to helping them strengthen their own criminal laws and then to developing international agreements in which they work with us. If they do not have the will, there is a limit to how much we can do.

One thing we do do throughout the world is try to get as many countries as possible to accede to the Convention on Cyber Crime, which we think is a very useful international framework, one that provides a very strong foundation for international cooperation in these cases.

Senator KLOBUCHAR. Now, I know a lot of my colleagues have asked you about resources and how that would be helpful. How about legal changes? Are there changes that we could make to current law? What would you have on your top list of things that would be helpful as we battle this new-found crime?

Mr. WEINSTEIN. Well, I can say that we have got some ideas about some potential changes to 1030 that we are discussing and working on, and as soon as they are done, we will be pleased to bring them to your attention and to work with you on them, as well as any other ideas that you have.

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00024 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

Obviously, we are watching and very eager to be engaged on the ECPA debate. I know you had a hearing on that where Mr. Baker and others testified last week because changes in ECPA actually—if standards are increased in such a way that puts information out of the reach of law enforcement, it makes it very difficult for us to investigate and prosecute cases against cyber criminals who threaten Americans' privacy. So we are very eager to engage in that debate.

And as you may know, there is an interagency process that is moving at a fever pitch to develop some cyber security legislation. I would not say it has been at a fever pitch throughout its life, but I can tell you that in the last 6 weeks it has.

Senator KLOBUCHAR. When did it start, Mr. Weinstein?

Mr. WEINSTEIN. It started a while ago.

Senator KLOBUCHAR. OK.

Mr. WEINSTEIN. The fever pitch started more recently.

Senator KLOBUCHAR. OK.

Mr. WEINSTEIN. But, you know, we have got people who are literally working around the clock, judging by the time at which they are e-mailing me in the middle of the night to try to get proposals ready to present to you, and so I think that will happen very soon.

Senator KLOBUCHAR. Are you satisfied with the criminal penalties in place for engaging in cyber crime?

Mr. WEINSTEIN. Well, one of the ideas we do have involves some streamlining and strengthening some of the penalties that are provided in 1030. As I said, that proposal is still baking, and when it is fully cooked, we will be pleased to bring it to you and talk to you about it further.

Senator KLOBUCHAR. OK. I am out of time here, and I will just ask in writing Assistant Director Snow questions about the work with the private sector. Minnesota is home to Target and Best Buy and several major companies that deal with this all the time, and so I am interested in that issue. I actually visited McAfee, their offices in Minnesota, and the work that is being done there.

And then I also will, for the record, Mr. Martinez, follow up on some questions with you as well.

Mr. MARTINEZ. Absolutely.

[The questions of Senator Klobuchar appears under questions and answers.]

Senator KLOBUCHAR. Thank you very much.

Chairman WHITEHOUSE. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

I would like to join in thanking Senator Whitehouse for holding this hearing and for his interest and effective action in this area.

You know, we have been talking a lot about enforcement and about potential changes in the law, and if I have time, I would like to return to that subject. But I was very interested in an observation made by one of the people who is going to follow you in talking to us today, John Savage, who is a professor at Brown, who says in his testimony, and I am going to quote, "Computer industry insiders have solutions to many cyber security problems, but the incentives to adopt them are weak, primarily because security is expensive and there is no requirement they be adopted until disaster strikes."

Now, I have been involved in enforcement relating to this issue, and I do not mean to minimize your efforts. In fact, I think they have been heroic and remarkably effective, both at the Federal level where you work and often at the State level. But don't the holders of this information—and I am thinking of Epsilon, for example, most recently the supposed victim of a major breach—have a greater obligation to do more to safeguard this information? And how do we create those incentives that Professor Savage mentions to make your job more effective? I will not say "easier" because nothing can make your job easier, and I have great admiration for what you do. But how do we create those incentives so that private companies are more partners of yours in this enforcement effort? And I ask that of all three of you, and I will let you go in whatever order you would like.

Mr. MARTINEZ. I will take it. Senator——

Senator BLUMENTHAL. And, by the way, you may disagree with Professor Savage, too. I am not assuming that you will necessarily agree.

Mr. MARTINEZ. Senator, I believe also Mr. Weinstein spoke about a proposed package that is forthcoming here to Congress regarding a comprehensive number of cyber bills that all three organizations sitting at this table have been involved in the crafting.

One of those proposals involves data breach legislation, and I think it is important for us to create a national data breach bill so that we do not continue to have this myriad of—I believe right now there are 47 individual State data breach requirements, all of which are unique and all of which have different reporting requirements. So I think it is important that we do have a national data breach bill.

As part of that national breach bill, I think it is incumbent and it should be required that if companies do have an intrusion, they not only notify the consumers or the victims whose information might have potentially been stolen, but that they also notify the Government and that the Government be notified of the fact that there has been an intrusion.

To the point of the professor's, the other part that I think is important in the legislation—and I think the administration is going to be addressing that—is that there also be a safe harbor for those computers that have protected the information in a proper way. So even though they have an intrusion but the information is protected, that they themselves be protected via some type of safe harbor so that civil action might not be taken.

I think in the package of legislation that the administration is finalizing, you are going to see all three aspects of that in that legislation.

Mr. SNOW. And, Senator, I would just add that I would echo Mr. Martinez's comments, and I would also say that I do not think anything in the professor's statement is wrong. I think the professor is exactly right. But a little bit closer scrutiny of this statement would say something that is really important, and that is that many of these people have many of the solutions for many of the problems and understand that it is a multi-layered, multi-faceted problem. To throw a few solutions at some of the problems does not solve all the problems. So we have to understand.

Right now I do not think there is any secure system out there. I think it takes a defense in-depth layering, and I think that is something that we have to work on.

On his point of weak incentives, I think he is exactly on point. You know, I will go back to the bank robbery days that the FBI was going from place to place. Just getting somebody to put in a new VCR was extremely difficult because that was 60-odd-some dollars at the time, and that did not do anything but take away from the security budget.

I think that is the same thing we see in businesses right now. That security that we layer that we think is essential is not really put in place until there is a tragic incident, an embarrassing incident, an incident that costs them close to a huge concern about them being a continuing entity or a going concern.

Senator BLUMENTHAL. Mr. Weinstein.

Mr. WEINSTEIN. I do not have anything to add to what Mr. Martinez and Assistant Director Snow said other than to emphasize that it has to be both incentives for companies to protect themselves against breaches—and I do think that most companies, especially those that operate in good faith and care about their business reputations, do want to protect themselves—but also, as Mr. Martinez said, to report the breaches when they do happen.

I anticipate, although the shape of our package of proposals is still being formed, but I do anticipate there will be something about data breach reporting in that package, and we look forward to working with you on that.

Senator BLUMENTHAL. Well, I would be eager to work with. As you may know, Connecticut is one of those States that has a reporting requirement. I have asked for Epsilon to provide credit reporting services as well as identity theft insurance, which has been standard in what Connecticut at least has asked the companies that had this information that may have been breached to do in the past and has also sought penalties. So I might just suggest, without commenting on Epsilon or any other particular instance, that providing these incentives for adoption of this technology is something that is worth your very serious and positive scrutiny.

Thank you.

Chairman WHITEHOUSE. We will go very shortly to the next group of witnesses, and I will excuse this panel. I do have a question for the record that I would like each of you to take with you and answer for me, and I think Senator Kyl will do his in writing.

Assistant Director Snow mentioned the high level of activity of the sort of eBay type situation of the Russian-based hackers and criminals who are working on this, and I am reminded of the lawsuit that was brought by Microsoft against the Waledac botnet, which was able to obtain a court order involving the legitimate Internet world—the domain providers, the ISPs and so forth—to cut off service from the command-and-control nodes of that botnet so that it no longer was operative. And it strikes me that without actually doing criminal prosecutions of folks, we could be very aggressively hunting down these criminals and these attackers on the Web and disabling them with civil injunctive measures that require the ISPs, the domain registers, and so forth to stop providing service in certain components or to certain addresses or to certain types

of transmissions from addresses. And because virtually all of this flows through the United States at some point, jurisdiction should be fairly easy to get compared to an unknown hacker who is working through a server in Estonia that links to a server in the Ukraine that links to a server somewhere else before it even gets here.

So I would like to hear from each of you as to what extent your organization's cyber resources are empowered to support an active criminal defense that uses civil law to shut down some of these activities by authorizing the service providers to engage with court permission, protected from liability because of that, in a way that disables this. OK. Clear?

[The information appears as a submission for the record.]

Chairman WHITEHOUSE. And Senator Kyl will do his for the record.

[The questions of Senator Kyl appear under questions and answers.]

Chairman WHITEHOUSE. So with gratitude for your service and for your focus on this very significant problem, I will excuse this panel, and we will take a 2-minute recess while the next panel convenes. Gentlemen, thank you all very much.

[Pause.]

Chairman WHITEHOUSE. Let me call the new panel to order, and thank you all for being here. Let me first ask that you stand and be sworn. Do you affirm that the testimony you will give in this Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Ms. SCHNECK. I do.

Mr. SAVAGE. I do.

Mr. BAKER. I do.

Chairman WHITEHOUSE. Thank you. Please be seated.

Welcome. We will begin with Phyllis Schneck, who comes to us from McAfee, where she is vice president and chief technology officer for their global public sector operations. Previously, she was vice president for threat intelligence for McAfee. She served as a commissioner and a working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security, which I am proud to say was a report co-authored by my colleague in the Rhode Island delegation, Congressman Jim Langevin. Ms. Schneck also served—Dr. Schneck, I should say, also served for eight years as Chairman of the National Board of Directors of the FBI's InfraGard program, which has already been mentioned today, and vice president of research integration at Secure Computing. She has a Ph.D. in computer science from Georgia Tech.

Ms. Schneck.

STATEMENT OF PHYLLIS SCHNECK, PH.D., VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR, MCAFEE INC., RESTON, VIRGINIA

Ms. SCHNECK. Chairman Whitehouse, Ranking Member Kyl, and other distinguished members of the Subcommittee, thank you for requesting McAfee's views on responding to the threat of cyber crime and cyber terrorism. Your Subcommittee is playing a vital

role in cyber security, helping to investigate sophisticated syndicates of criminals and terrorists who deploy cyber attacks to finance their operations and undermine the security of our country. Thank you for your commitment.

My testimony will focus on the following three areas: the evolution of the cyber security threat landscape, as that has changed over the past few decades; two major cyber security attacks—Operation Aurora and Night Dragon—McAfee's technical response to the cyber crime challenge and the implications for national security from those attacks and others that look just like it as we look at the future of our cyber security and resilience in this country; McAfee's commitment to partnering with law enforcement and the law enforcement community; and policy recommendations to support law enforcement and improved public-private collaboration and information sharing that is so vital to give the Government the capabilities that it needs to respond to this modern cyber security challenge.

First, a rollback on McAfee and our definition of cyber crime for this testimony. McAfee protects businesses, consumers, and the public sector worldwide from cyber threat. Headquartered in Santa Clara, California; Plano, Texas; and a large operation in Minnesota, McAfee is the world's largest pure dedicated cyber security company, and McAfee is a wholly owned subsidiary of Intel Corporation.

Today we use the term "cyber crime" to cover the act of using electronic means to gain unauthorized access. As we heard in the last hearing, cyber crime covers the spectrum, from simply gaining notoriety to pooling funds, for organized crime, now to intellectual property, and destruction—destruction of critical infrastructure—with the very far end of the spectrum some are calling "cyber terrorism."

Our overall key challenge is that the profit model benefits the cyber adversary: very low barrier to entry, this stuff is easy for them; and very, very strong reward, often large amounts of money; often destruction; very, very little attribution.

This adversary is fast. This adversary works faster than we do. They build relationships, they build trust. As was mentioned in the last hearing, the cyber underground, they know how to share information. They have no intellectual property boundaries, no legal boundaries, very often funded fully by their government. No problems to execution.

As we have evolved in the cyber security threat landscape, the traditional model of defeating malware, which is basically an instruction that commands a machine to do now whatever the adversary desires, and whenever, and send back whatever the adversary desires, our traditional signature model does not work.

For the past decade, the industry has looked at understanding what could come in, recognizing what is wrong, and blocking it, just like a vaccine would block a cold from your body or a disease.

So we look at 50,000 new pieces of malware every day in McAfee labs. We have seen many of the sites that were described earlier in the cyber underground. We track the criminals. We see this adversary, and we propose two key technologies that we believe are the future to cyber security technology on the technical side, under-

standing that this is half a people problem, half a technology problem. These key technologies are:

Whitelisting, which is very simply closing the door. If you are not an approved instruction, you do not run. It no longer matters how many bad-guy instructions are on a machine. If you are not known to be good, you simply do not run.

The second one being global threat intelligence, behavioral understanding to build the cyber immune system, just like your body fights off a cold or disease without knowing its name automatically, we believe our networks should be a lot smarter and pull data from our companies and others across the financial field and the energy sector, across the critical infrastructure to block bad things from coming into networks.

Two major attacks this year that McAfee led for investigation: Operation Aurora and Night Dragon. In January 2010, Operation Aurora was exposed for having compromised Google and 30 other companies. This year, Night Dragon.

In Operation Aurora, the adversary was looking for intellectual property. Very large stores of IP and software, and they identified exactly who in those companies would have it, and they got it by social engineering their way in and getting those people to answer an instant message.

In Night Dragon, they targeted the oil and gas industry across the world looking for architectural documents, pipelines, and looking at where the new oil exploration would occur.

McAfee is fully committed to partnering with law enforcement. We have a long history, my own having run the FBI's InfraGard program nationally on the private sector side for 8 years. I also chair the National Cyber Forensics and Training Alliance. My colleagues, thousands of them working in partnership with law enforcement every day at the Federal, state, and local levels, assisting with investigations, working closely with the intelligence community, also building strong relationships with the FBI and Secret Service across our partners.

We recommend in policy more budget to fund our law enforcement colleagues, greater situational awareness in this data, and stronger global partnerships, protect the private sector so that we can release data very quickly without worrying about material benefits for shareholders.

Thank you again for the opportunity to be a part of the process in fighting cyber crime with law enforcement and Government relationships. I look forward to your questions and continued discussion.

[The prepared statement of Ms. Schneck appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Dr. Schneck.

Before I go on to Dr. Savage, since you referenced the Night Dragon report, I would, first of all, like to compliment it. It is the clearest, most trenchant, accessible document I have yet read in a lot of reading that I have done about cyber security. Anybody who is watching this or listening to this and has not had a look at that, it is a really, really good document, both in terms of the overlay, the sort of contextualization of this as a rapidly emerging threat with rapidly increasing sophistication and multiplication of inci-

dents, but also as a quite clear layman's description of how the attack takes place right down to showing the screens on the computer that you would see as you go through the attack.

So what I will ask is unanimous consent that that report be made a matter of record for this Committee hearing, and we can provide a copy because I have got it. But I do applaud that. I think that is a very, very clear, useful document, and thank you very much for preparing that.

[The report appears as a submission for the record.]

Chairman WHITEHOUSE. Also, unlike most of the stuff that is put out here, it was unclassified and not kept proprietary. One of the real problems in this area is that we know so little about it because if it is the Government it is classified, if it is the private sector it is held proprietary, and the public is kept, unfortunately, ignorant of the actual threat. So I think you did a real service with that, and I thank you.

Ms. SCHNECK. Thank you, Chairman Whitehouse. Would it be out of line for me to point out that report was written by my colleague, Dmitri Alperovich, in the row behind me.

Chairman WHITEHOUSE. No, it would not be. It would be very appropriate, and I am glad that he is here for this. I guess I lucked out by saying nice things about it instead of bad things.

[Laughter.]

Chairman WHITEHOUSE. And now from the great State of Rhode Island, from a university we are very proud of, Brown University. I am delighted to have the chance to introduce Dr. Savage. He is a professor in the Department of Computer Science at Brown, currently conducting research on cyber security, computational nanotechnology, the performance of multi-core chips, and reliable computing with unreliable elements.

It sounds like something we try to do here in Congress.

Dr. Savage served as a Jefferson Science Fellow in the U.S. Department of State during the 2009–10 academic year. He earned his Ph.D. in electrical engineering at MIT, after which he joined Bell Labs and then the faculty at Brown where he co-founded the Department of Computer Science in 1979. He has multiple clearances and knows a lot about this.

Dr. Savage, thank you. Please proceed.

STATEMENT OF JOHN E. SAVAGE, PROFESSOR OF COMPUTER SCIENCE, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND

Mr. SAVAGE. Thank you, Chairman Whitehouse and Ranking Member Kyl and members of the Subcommittee.

As you have heard, the Internet which is so important to our economy, also exposes us to great risks. I have a few statistics that highlight this, fact. Last year it was reported that more than half of all the computers worldwide were compromised. This means that each of these computers is not only capable of being used to steal personal, corporate, or Government data; they can also be marshalled into botnets and used for nefarious purposes.

For example, the Mariposa botnet is reported to have controlled a remarkable 12.7 million computers, distributed across 190 countries, before it was silenced in early 2010. If a botnet of this size were used to launch a denial-of-service attack, it could wreak havoc

on the Internet. More importantly, if deployed to disrupt Internet routing tables using a technique discovered and announced in early February, experts say that routing on the Internet could be severely disrupted.

I cite these examples to illustrate some of the damage that could be done via the Internet. If we add to the mix that some important control systems, such as those used for electrical power generation, can also be attacked, destroyed, or disabled by the Internet, we see that hazards lurk here that were unanticipated when the Internet was designed. The Internet, which has contributed so much to our economic strength, allows us to more tightly integrate segments of our economy; thus, attacking the Internet is a way to attack large portions of our economy.

Because cyber crime and terrorism are international in nature, they both require a domestic and international response. We must elevate our domestic security standards in our hardware and software networks. We cannot tolerate having several times more botnets than any other nation, nor large numbers of compromised computers. We also need to better control the supply chain as well as strike international agreements to curb abuses that originate at foreign sites.

So we ask: What steps can we take as a Nation?

First, we should create the incentives and, if necessary, regulations to design and improve computer security. Any proposed regulations should be developed through a consultative process involving those being regulated.

Second, the private sector and individual citizens need to be educated to the need to keep their systems current with security standards.

Third, steps should be taken to make the domain name system more robust by accelerating the adoption of the domain name system security extensions.

Fourth, understanding that our Nation faces a serious deficit, we must nevertheless maintain strategic and targeted funding for cyber R&D. In the policy dimension, we should engage in a national conversation on the types of international agreements that will best serve our cyber security interests. Many interesting ideas have been proposed that should be debated. Leading thinkers have said that the U.S. is not sufficiently engaged in international negotiations to our detriment.

Some may ask: Can we manage these problems? Are these problems manageable? My answer is yes. I liken our computers to our homes. A determined attacker can easily break into them. So why aren't most of our homes invaded more often? Apparently because the locks are good enough, the neighbors sufficiently vigilant, uniformed police officers are sufficiently visible, and the punishment if caught and convicted sufficiently onerous to deter attackers. We need to arrive at a similar state in cyberspace.

Many of us are struggling to understand, from both policy and technological points of view, these issues. There are few technologists conversant with policy and few policymaker sufficiently knowledgeable about technology. Thus, there is an opportunity here to bring the two camps together.

In the early days of the cold war, strategy development is said to have lacked sophistication. However, once the insightful analysts studied the issues, a more mature approach to policy emerged. The same must be done for cyber security policy.

In closing, let me say that cyber security research is very young. While some profoundly interesting results have been developed, many challenges remain. Since cyber security plays a central role in our economy and is an important branch of national security, it deserves to be given priority for strategic, targeted research funding in both the technological and policy realms.

Thanks, and I am happy to answer your questions.

[The prepared statement of Mr. Savage appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Dr. Savage.

Our final witness is Stewart Baker, a partner in the law firm of Steptoe & Johnson, where his practice covers national and homeland security, cyber security, electronic surveillance, law enforcement, export control, encryption, and related technology issues. From 2005 to 2009, Mr. Baker served as the first Assistant Secretary for Policy at the Department of Homeland Security, where he oversaw the office responsible for department-wide policy analysis, international affairs, strategic planning, and relationships with the private sector. From 1992 to 1994, Mr. Baker was General Counsel of the National Security Agency.

Thank you for being with us.

STATEMENT OF STEWART A. BAKER, PARTNER, STEPTOE & JOHNSON, LLP, WASHINGTON, D.C.

Mr. BAKER. Thank you, Mr. Chairman, Ranking Member Kyl, Senator Blumenthal.

I should say the one other credential that was left off of my biography is that I am Brown Class of 1969.

Chairman WHITEHOUSE. Very important credential to the Chairman. Thank you.

Mr. BAKER. I would like to spend a little time on—I talked in my testimony about how bad this problem is. It is worse even than we have heard today because there really are very few barriers to a substantial increase in cyber attacks and cyber crime. I laid out in my testimony the many things that we had hoped will save us that will not.

Blaming Microsoft is not going to save us because almost all of the software that is being used today has similar flaws. Trying to use tokens, which many of us believe would save us instead of passwords, increasingly have been compromised by hacking attacks and by realtime exfiltration of those token credentials.

We are not even going to be able to save ourselves if we call people up and say, "Did you really send me this e-mail?" Because that kind of out-of-band confirmation of the sort you get with your credit card is increasingly at risk as we move to IP telephony, which will have all of the problems that ordinarily computers have as well.

Disconnecting from the Internet, which we also are not going to do, is not going to solve this problem because the agencies that have tried doing that—the Defense Department, the Iranian

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00033 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

Natanz centrifuge plant—have, nonetheless, been compromised by attacks that use thumb drives and other media as a way of transporting the compromising software.

What many of us hope to rely on, the anonymity that nobody is really particularly looking for me, is also not going to save us because, increasingly, it is possible to essentially infect the world and then ask your malware to run in the background until you do something that the crooks think is interesting, like log on to a particular account with a private equity fund, which indicates you have enough money to be worth stealing from, at which point they will start stealing from you.

All of those things are solutions that will not actually work. And perhaps most important for this Committee and this hearing, law enforcement is, in my view, almost entirely helpless at this point. Six more prosecutors are not going to address this issue in any significant way, and the principal reason for that is that—I thought Professor Savage got it right. We do feel safe in our houses, but it is not because the locks are perfect. The locks on our houses are much worse than the locks that are already on our computers. What is different is that there is a realistic possibility of being caught committing a crime if you try to break into somebody's house and almost no possibility that you will be caught and prosecuted if you commit a cyber crime.

I have suggested a bunch of rather tentative approaches to solutions in my testimony, but I would like to just focus on one, which is we really need to do a much better job of building in attribution and minimizing anonymity on the Internet, making it much more difficult for people to do business, send e-mails, transmit packets and the like, and be confident that they cannot be tracked back to their actual identity.

This is a very difficult task. It is an architectural problem that is quite significant. But, in my view, we will not solve this problem if we cannot realistically threaten to punish the people who are carrying these attacks out. We will simply see more and more sophisticated, more and more elaborate, and more and more damaging attacks until we begin structuring the Internet and structuring the relationship that ISPs have with each other and with their customers so that it is much more difficult for people to avoid being identified when they commit these crimes.

I will stop there.

[The prepared statement of Mr. Baker appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much.

We had General Alexander, who I think is a really remarkable individual, come to the University of Rhode Island yesterday. He came at the invitation of Congressman Langevin, who has a very significant role in this area on the House side, and Jim Langevin and I talk frequently about this issue because I have an interest on our side as well.

During the course of the discussion, General Alexander said that we could—right now our stock markets, our financial markets could be taken down, our power grid could be taken down. If our power grid were taken down, it would not come up quickly. It would not be just like the branch fell on the wire outside your

house, but do not worry, when the truck comes, the power will be back on. It would be much more persistent and prolonged than that. He said that the entire financial sector is vulnerable and could be compromised, communications networks, and that they could interlock. So the scale of how bad this could be, if it really gets to the level of full-blown cyber war, is really very, very dramatic.

I am interested—since we have private sector folks here, this may seem like a hypothetical question, but I would love to get your take on it.

If you imagine that there is a universe of cyber threats out there and within that universe of cyber threats there is a group of them about which the Government has awareness—Mr. Baker, your old shop has pretty wide awareness, probably wider than anybody else in the world, into the criminal ecosystem of the cyber world. Within that larger awareness, there is an awareness that the private sector has at its best level, at the level of McAfee, at the level of Symantec, RSA, and so forth.

I would love, starting with you, Dr. Schneck, to get your sense of what portion of the awareness that NSA has of the cyber threat you think the private sector has. Clearly, it is going to be a subset. But is it a tiny subset, or is it a significant portion? What is your guess on how much visibility McAfee and Symantec and the rest of the private sector defenders of our private sector corporations have compared to the NSA and to the overall picture?

Ms. SCHNECK. Thank you, Chairman Whitehouse. I will steal some words from AD Snow earlier and ask that we could continue part of this answer in a different forum. So clearly there will be an overlap between what any Government entity, whether it is intelligence, community law enforcement, DHS—would know and what the private sector knows. I think we get our intelligence differently in some cases. We gets ours from protecting customers, so first and foremost, whether the threat is just to get a little money or whether it is to destroy the electric grid, we block that threat. We stand in front of the target; we make sure the threat does not get there. That is our first move. That is the in-line, speed-of-light work.

The second line is the human work. The reason that is so hard is because we see all this data come together, and it paints a picture. This happened in Night Dragon. And as that picture came together, you realize that it is targeting the oil and gas sector. At what point can we in the private sector share that picture with the intelligence community, with the FBI and the Secret Service?

Chairman WHITEHOUSE. Let me try to focus back on my question, and before I give the other two witnesses a chance to answer it, would you at least concede that the awareness that the cyber defense private sector community has of the threat is significantly smaller than the awareness that NSA has of the threat?

Ms. SCHNECK. So it is hard to answer that question in this forum. I think the awareness is different. I do believe there is an overlap. I think there is a lot of data in the private sector that, if we were able to share that more readily with some legal protection, we would protect our country better.

Senator Whitehouse. Do you understand my question, Dr. Savage——

Ms. SCHNECK. I do, and I believe——

Chairman WHITEHOUSE. No, no. I am sorry. I am going on to the next witness.

Ms. SCHNECK. OK.

Mr. SAVAGE. I do understand your question, and I cannot answer it either because I do not represent either the private industry or the intelligence community.

However, what I will say is I would not be surprised if the private sector had access to perhaps more data than the National Security Agency simply by virtue of the fact that have sold, they sell products to customers worldwide, monitor the state of computers worldwide. Although before I do not know for sure, I expect that the National Security Agency has a different focus.

So I would not be surprised if the private sector had a great deal of very useful information.

Chairman WHITEHOUSE. And, Mr. Baker, what is your take?

Mr. BAKER. I would divide the problem into three possible kinds of attacks: there are attacks to steal money, there are attacks to steal secrets, and there are attacks to sabotage a system.

When it is a question of stealing money, I would say the private sector is better informed and better protected than the U.S. Government or Government agencies generally. It affects the bottom line. They know how much to spend. They want to spend enough to stop losses that are equivalent to what they have spent. And they do a better job than the U.S. Government protecting themselves from that kind of an attack.

Stealing secrets, I would say the U.S. Government has a better awareness and, by and large, I get more calls from people in the private sector who are alerted to their losses by the U.S. Government than the other way around. And there is a tendency, if you do not steal secrets for a living, as intelligence agencies do, not to believe that people are really doing that to you, and the private sector falls prey to that illusion.

And then there is sabotage where I think the private sector is utterly clueless. They do not want to think about the possibility of sabotage because they have no idea what to do about that. They will end up spending money and getting nothing obvious back because they are running now—they have not been sabotaged yet, so all they get is a sense that maybe they would withstand an attack, but they do not even know that.

And so they are reluctant to spend money or even to hear the message in the private sector, the electrical grid, or the pipeline companies and the like. The reluctance to hear that message is profound.

Chairman WHITEHOUSE. Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

First, Mr. Baker, two questions for you. You discussed the supply chain vulnerabilities, including the new smart grid infrastructure. What is being done to ensure that the smart grid does not become in essence an electronic Trojan horse?

Mr. BAKER. Well, some things are being done on paper. There are security standards being developed. Whether they are really suffi-

cient is open to question. But even if they were sufficient, there is not an obvious enforcement mechanism. The mechanisms for regulating power companies are deeply local and State, and both the power companies and the State PUCs like it that way, and they do not want the Federal Government to step in and start telling them anything about their business. And so while the Federal Government can recommend some security standards, the PUCs who have to enforce them, in my understanding, are not really doing much.

Senator KYL. So we have still got a big problem there.

Mr. BAKER. Yes.

Senator KYL. Now, I think you are aware that last year Congress gave the Department of Defense some new powers to protect its information systems, and I wonder—regarding the supply chain, again. I am just wondering whether you think maybe Congress should use that kind of authority as a template for other agencies in the Federal Government.

Mr. BAKER. Well, certainly other agencies beyond the Defense Department have to worry about the possibility that the supply chain will compromise them, and indeed, you know, anything that we think is a worry for the Defense Department is probably a worry for the New York Stock Exchange or Citibank, and we should not be encouraging them or allowing them, without knowing about the risk, to continue to rely on insecure material.

Senator KYL. So we might take a look at that template in dealing with other agencies that have important issues like that.

Mr. BAKER. Yes.

Senator KYL. Now, for all of you, there is a sense here that there is no silver bullet except better enforcement, but better enforcement is really hard to do, well, primarily from a resource standpoint, but also a capability standpoint. So I presume that incremental changes, including creating incentives, is one of the answers here. And in terms of changing behavior, my question is with the private sector—in particular business but also individuals—whether a greater use of the concept of insurance as providing incentives would help the private sector develop better protections. Maybe we will start with you, Mr. Savage, and then Phyllis.

Mr. SAVAGE. I agree. Cyber insurance to protect against fraud, theft, interruption of service, things of that sort would be very valuable, because I recall many years ago learning about workers' compensation insurance where an insurance company would issue a policy but they would also provide experts to come into your place of business to help you improve it so that they could reduce the number of injuries and, therefore, the number of charges.

When I was in the State Department, I sat on a NITRD panel that put together a set of recommendations, one of which was a cyber economics recommendation for funding in fiscal year 2012s budget, and the idea there being that if you offer insurance, you can invite companies who are going to purchase the insurance to provide you with incident information, which you can then collect and use to create actuarial tables reducing their costs, but also pooling these resources with other insurance companies.

The good news is that when I was in the State Department, I received a call from a Brown grad who had seen I was a Jefferson Science Fellow. She works for an insurance company in the Hart-

ford area that sells insurance of this kind, but they were at a little bit at sea because they could not really find the others and work with the others to do this kind of thing that I described.

Senator KYL. Especially ways to help resolve that problem and whether the Government should be involved in this, Dr. Schneck?

Ms. SCHNECK. So, thank you. We have looked at the insurance model for about 11 years that I remember. The key road block to that was the lack of the actuarial data, to Professor Savage's point on the need for that data. So in the startup, we have plenty of data we can look back on in driving habits and other areas where things are insured, but in this arena so little is reported that we know what we know because we are out there protecting, but to Mr. Baker's point, most of the private sector does not have this kind of knowledge. So that actuarial data to make the model work on the insurance would be exceedingly difficult.

That is not to say it would not be a great idea to incentive, but we would have to make sure of two things: one is that the data is there so that nobody gets burnt, so the model fits; and the other is to ensure that we are not encouraging companies to be compliant, they have to be secure. There is a very big difference. Do not just check the box, but comprehensively protect your infrastructure.

Senator KYL. Mr. Baker, any other thoughts?

Mr. BAKER. Yes, very briefly. For insurance to work, people have to either expect a harm, an identifiable harm, or identifiable liability. The likelihood of liability in this area has so far been pretty minimal just because of the difficulty of tracking the attacks. And if all they steal is secrets, you are not going to be able to identify a harm that an insurance company will be comfortable reimbursing you for.

So it is part of the solution, but it is not as good a solution as I would like.

Senator KYL. Thank you.

Chairman WHITEHOUSE. Senator Blumenthal.

Senator BLUMENTHAL. Thank you. I would like to pursue that line of questioning, but first thank you, all three of you, for your very enlightening and useful testimony, and I would like to pursue some of the questions here outside the time that I have.

But in terms of liability, that is something that corporations understand. If we talk about incentives, which is where I was going with the last panel—treble damages—we know how to impose liability, we know how to penalize. The courts do it all the time. They have to put estimates on that harm. It may be difficult to calculate, but, you know, we do it with pain and suffering. If we can do it with pain and suffering, then we can do it with the kind of commercial damage that people suffer, which is much easier in many respects to quantify.

So for all of you—but it is a question raised by Dr. Savage's testimony, and I am quoting again: ". . . the incentives to adopt them are weak"—referring to the solutions to these cyber security problems—"primarily because security is expensive and there is no requirement they be adopted until disaster strikes."

What can we require—and I invite you to supplement your answers here perhaps after you think about it some more. What can

we require, whether it is liability or Senator Kyl mentioned insurance—and I agree with you about all the difficulties raised by the insurance model. What can we do to really grow your business, Dr. Schneck? And I do not mean that altogether facetiously, I mean not just grow your business, but grow the interest and incentive to do the kinds of things that you advise your clients to do.

Ms. SCHNECK. Thank you. I think the first might be to incentivize some innovation. So we have grown by finding ways around this adversary. We get them by going at the speed of light. That was a focus of necessity. That was market driven.

If we can change our culture a bit to have companies incented to innovate around security and find models that work, find ways that make them money by being more secure—and the insurance models is a subset of that—I think that is one area.

The other might be some tax incentives, and, again, not just being compliant but in doing it right and having that—again, the decade-old discussion but the top-down policy, the culture of security in the company.

Senator BLUMENTHAL. But we want to measure results, not just that they put a better fence around the home——

Ms. SCHNECK. Correct.

Senator BLUMENTHAL.—or a better fire alarm—which, by the way, insurance companies do reward so the insurance model does work—or other kinds of alarms on homes.

Professor Savage or Mr. Baker.

Mr. SAVAGE. I will say quickly, I continue to be troubled by end-user licensing agreements which state that the company selling me the software has no responsibility for it once it is in my hands. I cannot fix any bugs that exist or any security hazards that exist in that software myself. I cannot even keep it up to date quickly enough because, as we know, as we have heard, half of all the malware goes undetected.

It is said that last year PandaLabs reported that half of the malware lived for 1 day. I am not sure to what extent that statement is correct, but that is what I read.

Coming back to a point you made earlier, you asked about the technologies that could be incorporated, well, there are—you know, research is being done all the time, and it takes time, of course, for these results to appear in products. But there are ways to detect botnets. There are ways to defeat denial-of-service attacks and things of that sort. And if there were the right incentives—and I do not know what they are—maybe some of our companies would be more ready to adopt them.

Now, having said that, there has been a lot of work done by a number of companies both in the software sector and financial services sector to introduce security techniques to teach their engineers to write code that is less easily attacked. And I think many of those efforts are actually terrific, and you can see it, I think, in the reporting rates of errors.

So I want to applaud the industry for doing that. At the same time, I think they need to take responsibility for this issue. And as I say, many are, but not all.

Senator BLUMENTHAL. Thank you.

Mr. BAKER. If I could just—I know you are deeply familiar with the data breach laws and the penalties for that, and I have good news and bad news about those laws.

The good news is they have made a big difference in corporate behavior. The companies do not want to have to disclose that they have released a large amount of personal information about consumers, and they will take steps to prevent that from happening.

The bad news is that that is where the security budgets have, by and large, gone. They are spending a lot of money to make sure that their hard drives are encrypted so that if they leave the computer, the laptop, at the airport, they do not have to disclose a breach. They are not, by and large, treating some of these more sophisticated attacks with the same kind of attention because they do not tend to produce a verifiable personal information breach.

And so if you are going to go down that road, I would urge you to try to find an agency with a broader picture of the kinds of attacks that can adjust the incentives so people are actually responding to the worst kinds of attacks, the ones that are most dangerous to us as a country.

Senator BLUMENTHAL. Thank you.

Thank you, Mr. Chairman.

Chairman WHITEHOUSE. Mr. Baker, as the lawyer on the panel, let me ask you two questions.

One, in response to what Dr. Savage said, should we be concerned that significant players in this area are purporting, at least, in their contractual arrangements to relieve themselves of any liability, given that liability is often a motivating factor in human behavior?

And, second, to follow up on my question to the earlier panel, I was very impressed by Microsoft's lawsuit. I asked them to send me the complaint. I thought it was very well done. And they did not really have a hostile defendant. The defendant, the provider who was at stake, was perfectly happy to comply as long as they had a court order that gave them a reason to do it and protected them from any liability for what they did. And I am a little bit surprised that there does not seem to be more activity in that arena, somebody knows that there is a bot out there that they can disable, somebody knows that there is a worm out there, somebody knows that there is a piece of—a website that is—you know, whatever it is that they know about their risk posture, it seems very rare that somebody actually goes to a court and says, oh, by the way, let us bring in—again, the domain registrar, their ISP, or whoever—and say we want you, because of the threat to our welfare here, to make this change in your programming so that our threat is diminished. And then everybody sits around and says yes, the judge hits the gavel, everybody is happy. It seems to me to be—the Microsoft thing does not seem to be repeating itself as often as I would have expected. I am aware of a couple of others, but that seems to be the breakthrough one, and it does not seem to have created the sort of torrent I expected of people going out to the courts, to the ISPs, to the domain registrars, to help them clean up the environment.

Mr. BAKER. Microsoft is in the unique position of seeing attacks around the world on their software and having the resources to

pursue creative solutions. And I agree with you, that was a very creative and constructive approach.

I do think that it is worth exploring what could be done to allow companies that have an interest in doing more but need some reassurance that what they are doing is not going to result in liability. One of the great values of a civil injunction and a civil order is that you know that the people that you are going after are not going to turn around and file lawsuits against you, because you have already gotten prior approval. And finding ways to relieve ISPs, other companies, of their fear that doing the right thing will result in liability is worth looking at. I think that is a constructive approach.

By and large, using the tort system to improve security is a pretty backward-looking approach; that is to say, by the time you get a judgment, you are 6 years past the problem, and it is probably——

Chairman WHITEHOUSE. You are back to my first question.

Mr. BAKER. Yes, I am coming back to your first——

Chairman WHITEHOUSE. Yes, I am not sure it is the best way——

Mr. BAKER. So I——

Chairman WHITEHOUSE. I am also not sure that allowing a company to completely relieve itself of liability contractually is very helpful in this space either, because it takes their mind off it and they go on to other projects.

Mr. BAKER. I do not disagree with you on that, and I support the idea of having at least agencies that understand what good security practices are, start to define those for companies, including software companies, to make sure that they are actually doing the things that they need to do. And if they say you need to do this and then the company does not do it, I do not think those contractual clauses are going to save them from liability.

Chairman WHITEHOUSE. Senator Kyl?

Senator KYL. Thank you very much.

Chairman WHITEHOUSE. Anything further?

Senator BLUMENTHAL. No. Thank you.

Chairman WHITEHOUSE. All right. We will conclude this hearing. I thank all of the witnesses, and once again I very much appreciate the Night Dragon report that McAfee did.

The hearing will stay open, the docket of the hearing will stay open for an additional week, and we will, of course, ask all of the witnesses to comply with the questions for the record that you will get in writing.

Again, thank you very much. This has been instructive and helpful.

The hearing is adjourned.

[Whereupon, at 4:33 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

VerDate Nov 24 2008 13:23 Dec 21, 2011 Jkt 071412 PO 00000 Frm 00041 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71412.TXT SJUD1 PsN: CMORC

QUESTIONS AND ANSWERS

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime &Terrorism
April 12, 2011

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I've been following this issue very closely and would appreciate learning your views on some the legislative proposal that are pending? What are some of the issues we should avoid and others we should embrace?

Stewart Baker Response:

In general, I believe that the Collins-Lieberman approach to regulation is the best compromise between laissez-faire and traditional regulation. That approach would allow DHS to challenge the private sector to come up with its own plans, but would reserve for DHS the right to demand more in response to particular threats (or a failure of responsibility by the sector in question).

I would also like to raise one other legislative proposal that raises cybersecurity concerns and falls squarely within Judiciary's jurisdiction. James Baker of the Justice Department recently testified to the Senate Judiciary Committee about ECPA reform, and in the process he touched on the provision of ECPA that prohibits ISPs from sharing subscriber data with the government in the absence of a court order. Mr. Baker hinted that this provision should perhaps be expanded to restrict ISPs from sharing subscriber data with third parties, at least where a commercial purpose is present:

A sixth potentially appropriate topic for legislation is the disclosure by service providers of customer information for commercial purposes. Under § 2702(c)(6) of ECPA, there are currently no explicit restrictions on a provider disclosing non-content information pertaining to a customer or subscriber "to any person other than a government entity." This approach may be insufficiently protective of customer privacy. Congress could consider whether this rule strikes the appropriate balance between providers and customers.

http://www.wired.com/images_blogs/threatlevel/2011/04/bakerepca.pdf

This strikes me as a dangerous step from the point of view of cybersecurity. Let me give one example. In a distributed denial of service attack, infected consumer machines are instructed to send packets to a victim site, which is then overwhelmed by malicious traffic. An ISP can often tell which of their customers' machines have been infected just by looking at the nature of the signals the machines are sending. If the ISP passes that information on to the victim site, the victim site or its service provider can shunt aside or drop signals from the infected computers as part of the target's defenses. This is just one of many ways in which it may be important for cybersecurity reasons to have quick, unimpeded sharing of information about subscribers who are engaged in activities that endanger others on the Internet.

Mr. Baker's casual proposal to extend the ECPA bar on disclosure would discourage such defensive moves. Before giving weight to Mr. Baker's views, Judiciary Committee should demand a formal, cleared legislative proposal from the administration, and it should look carefully at the security consequences before taking action on any such proposal.

RESPONSES OF PABLO MARTINEZ

Questions for the Record – Senator Sheldon Whitehouse

To Pablo Martinez, Deputy Special Agent In Charge, Criminal Investigation Division, Cyber Crime Operations, United States Secret Service.

Question:

Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Response:

In conjunction with our cyber security responsibilities, the Secret Service has no such civil enforcement authority.

Questions for the Record – Senator Dianne Feinstein

Question:
In your testimony, you note that in fiscal year 2010 you opened 957 criminal cases and arrested 1,217 suspects for cyber crime violations.

Can you provide, for each of the last five years:

- **The number of arrests for cyber crime offenses of individuals located in Russia?**
- **The number of individuals located in Russia prosecuted for cyber crime offenses?**
- **The number of arrests for cyber crime offenses of individuals located in Eastern Europe?**
- **The number of individuals located in Eastern Europe prosecuted for cyber crime offenses?**

Response:

The Secret Service submits the following information in response to the questions listed above:

Fiscal Year	Cases	Arrests	Number of individuals prosecuted in Eastern Europe	Number of individuals prosecuted in Russia
2010	957	1217	44	8
2009	936	1224	45	6
2008	846	1155	11	2
2007	961	789	11	8
2006	934	828	8	9

Questions for the Record – Senator Orrin G. Hatch

Question: (Snow/Martinez) National Cyber Investigative Joint Task Force

Mr. Snow and Mr. Martinez, hackers can simultaneously attack our critical infrastructure.

These hacks impact banking systems, electrical grids, transportation systems and military networks.

However, based on our organizational structure, the responsibility for defending these systems falls to a variety of different agencies. This could give the hacker an advantage unless information is shared.

I am aware that the FBI leads the National Cyber Investigative Joint Task Force. This national center has personnel from a variety of agencies and entities assigned there, including the Secret Service.

What is the dynamic inside the task force? Are agencies cooperating with one another?

Response:

The Secret Service maintains an excellent relationship with the Federal Bureau of Investigation. As one of the four core members, the Secret Service has one full-time agent assigned to the National Cyber Investigative Joint Task Force (NCIJTF). The Secret Service, through this liaison, provides investigative coordination and de-confliction with the NCIJTF partner agencies to improve the Nation's security against the full spectrum of cyber threats. Furthermore, through our participation, the Secret Service is able to share pertinent information related to evolving methodologies and operational strategies to counter criminal and nation-state cyber threats to the national information and financial infrastructure.

For example, during the recent intrusion of the Nasdaq, the Secret Service was able to share information with the FBI and other members of the NCIJTF that benefited the efforts undertaken in the investigation.

Additionally, as a part of the Secret Service's efforts to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following Department of Homeland Security (DHS) and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section

- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

Question: (Martinez) Secret Service National Computer Forensics Institute

Mr. Martinez, your testimony discussed the National Computer Forensics Institute located in Hoover, Alabama. I am aware that this center is utilized to train state and local investigators as well as prosecutors and judges in techniques relating to digital evidence and computer forensics.

1) Currently, how much funding does the Secret Service receive in its annual budget to operate the National Computer Forensics Institute?

Response:

The Secret Service does not receive direct funding in its annual budget to operate the National Computer Forensics Institute (NCFI). Currently, the Department of Homeland Security, via the National Protection and Programs Directorate (NPPD), is providing the Secret Service with $4 million in annual funding through an interagency agreement.

2) Is the allotted budget amount at a sufficient level to expand and grow the institute at a rate commensurate with growth of cyber crime cases investigated?

Response:

The current funding of $4 million per year only allows the NCFI to operate at 25% capacity.

3) Would additional funding of the NCFI, and for that matter the ECTFs, enable the Secret Service to maximize outreach to state and local investigators as well as provide more training opportunities for judges, prosecutors and detectives?

Response:

Additional funding would allow for the Secret Service to train additional state and local investigators, judges, and prosecutors through the NCFI. Further, the demand continues to increase due to the lack of accessible training offered to state and local officers, judges, and prosecutors.

For example, in 2010, the Secret Service was only able to accept 23% of all applicants. Operating under the same budget, in 2009, the Secret Service was only able to accept 25% of all applicants. It is important to note that the demand for training continues to increase. Additional funding would also allow for the NCFI to develop curriculum which would meet the demands for training to mitigate against current-day cybercrimes.

ECTFs are the backbone of the Secret Service's ability to fight cyber crime and have been recognized as an established program that is focused on preventing, detecting, mitigating, and investigating cyber attacks against the critical infrastructure of the United States. The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs, which are primarily funded through the Treasury Executive Office for Asset Forfeiture (TEOAF), includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners.

While the ECTF model has demonstrated its value to the Department of Homeland Security's mission of securing this nation's critical infrastructure, the current workload for each is substantial and there is a need for additional ECTFs. The Secret Service is committed to following the direction of Congress, as well as the goals set forth by the Department of Homeland Security, in attempting to enhance and expand programs that are designed to protect and defend America's critical infrastructure.

Question: (Martinez) Secret Service Presence In Future Countries of Cyber Concern

Mr. Martinez, are there countries or regions abroad that the Secret Service has determined to potentially be the future source of cyber crime directed at United States entities or businesses? If so, what countries or regions would the Secret Service like to establish a presence in an effort to train indigenous law enforcement and thwart the development of this nation into a cyber crime haven?

Response:

At no time in history have the challenges been greater for law enforcement. Technological innovations such as e-commerce, on-line banking and trading, the Internet, and electronic payments systems facilitate business but also remain prime targets for organized criminal groups. In recent years, there has been a significant increase in transnational criminal groups that target U.S. banking and other related financial interests.

Joint investigations with our foreign law enforcement partners have resulted in the arrests of hackers who have compromised financial institutions and conducted network intrusions into the Federal Reserve Bank, as well as those who traffic in stolen information. These investigations are made possible by the partnerships our existing offices have forged with their counterparts in law enforcement. Existing partnerships will be strengthened and new partnerships will be forged with an increase in Secret Service presence in offices around the world.

Cyber criminals remain active in Eastern Europe. The Secret Service is in the process of establishing a TDY presence in Ukraine to work with members of the Security Service of Ukraine (SBU) in cybercrime matters. The Service would also like to bolster the number of personnel currently assigned to some of its European offices to combat the threat from cybercrime.

The Secret Service sees a need to enhance and expand our overseas offices by 9 FTEs. This would allow for the Secret Service to permanently staff the Serious Organized Crime Agency (SOCA) Task Force in London, England, and add staff to several foreign offices. SOCA is one of the Secret Service's closest foreign law enforcement partners in the area of electronic crimes. Many of the cases under investigation by the SOCA have targets in common with Secret Service investigations. The Secret Service currently has agents detailed to SOCA and has day-to-day interaction with SOCA officers on cyber investigations in the United Kingdom and the European Union. Permanently staffing SOCA will enhance the ability of the Secret Service to protect U.S. financial interests.

Questions: (Martinez) Authorities and Tools

1) Mr. Martinez, are there any additional tools that the Secret Service requires to combat cyber crime both domestically and abroad?
2) Are there any titles or authorities that need to be updated to best meet the investigative demands of the Secret Service both domestically and abroad?

Response:

The effective relationships we have developed with our international law enforcement partners are attributed to our long-standing commitment to work with the host nation in a cooperative environment. This environment fosters relationships built on trust and mutual respect, and results in the sharing of information and best practices.

The Secret Service has established and supports Vetted Anti-Counterfeiting Forces (VACF) in Colombia. Since 2001, our vetted partners in Colombia have seized over $262 million in counterfeit U.S. currency, arrested more than 665 suspects, suppressed 113 counterfeit printing plants, and reduced the amount of Colombia-originated counterfeit passed within the United States by more than 70 percent.

Breaking up criminal networks required a highly coordinated law enforcement approach focused on constant innovation in tactics to meet emerging threats. The Secret Service believes that the vetted task force model would lend itself to combat cybercrime, as well. Identifying, training, and equipping cyber criminal investigators from foreign law enforcement agencies would assist the Secret Service in the investigation of cyber criminals located overseas.

The Department of Justice has made several recommendations to the Administration on Cyber Legislation that is being proposed as part of a comprehensive cyber legislative package. The Secret Service supports Department of Justice's proposals for enhancement of 18 USC 1030.

Questions for the Record – Senator Amy Klobuchar

Question: I was interested to read your testimony's discussion of "carding websites" that serve as forums for bad actors to buy and sell personal financial information among other activities. Are there any additional tools the Secret Service needs to combat these carding sites?

Response:

The Secret Service established the Cyber Investigations Branch, within the Criminal Investigative Division, to combat the rise in cyber crime targeting our nation's financial payment systems and critical infrastructures. The Cyber Investigations Branch is comprised of several important sections focused on investigating and preventing cyber attacks, including the Cyber Intelligence Section (CIS).

The CIS serves a critical investigative support function; it collects, analyzes, and disseminates data in support of Secret Service investigations nationwide and overseas and generates new investigative leads based upon this criminal information. Furthermore, CIS has developed an investigative unit. It is this unit that actively targets "carding" web sites. They work to identify, locate, and apprehend international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes, and have directly contributed to the arrests of 41 transnational cyber criminals.

The Secret Service has had tremendous success with its CIS investigative unit, and is hoping to expand its program by hiring, training, and equipping additional analysts with a specific expertise in Eurasian criminal organizations who use the Internet to carry out fraud schemes affecting the critical financial infrastructure of the United States. These analysts would be proficient in Eastern European languages (to include Russian, Polish, and Ukrainian), and Vietnamese.

Furthermore, as cyber criminals continue to explore and employ new technologies, commercial vendors are finding it harder to update their products to address advances among cyber criminals. As a result, law enforcement has turned to custom-built or specialized tools to supplement and complement their investigative approach. The Secret Service is also seeking additional resources to acquire tools to enhance its forensic capability to deal with the growing problem of cryptography, the encryption/decryption of data contained within a computer's hard drive.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 17, 2011

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Gordon M. Snow, Assistant Director of the Cyber Division at the Federal Bureau of Investigation, at a hearing before the Committee on April 12, 2011, entitled "Cyber Security: Responding to the Threat of Cyber Crime and Terrorism." We apologize for the delay and hope this information is of assistance to the Committee.

Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the April 12, 2011, Hearing Before the
Senate Committee on the Judiciary
Regarding Cyber Security: Responding to the
Threat of Cyber Crime and Terrorism**

Questions Posed by Senator Feinstein

1. In your testimony, you note that in 2010, FBI arrested a record 202 individuals for [cyber] criminal intrusions, up from 159 in 2009. You also testified that on the criminal side a majority of the attacks come from individuals located in Russia and Eastern European countries. Can you provide, for each of the last five years:

a. The number of arrests for cyber crime offenses of individuals located in Russia?

Response:

Year	Number of Arrests
2006	3
2007	0
2008	1
2009	1
2010	2

These responses are current as of 6/14/11

b. The number of individuals located in Russia prosecuted for cyber crime offenses?

Response:

Year	Number of Prosecutions
2006	0
2007	3
2008	0
2009	1
2010	1

c. The number of arrests for cyber crime offenses of individuals located in Eastern Europe?

Response:

Year	Number of Arrests
2006	38
2007	37
2008	109
2009	81
2010	149

d. The number of individuals located in Eastern Europe prosecuted for cyber crime offenses?

Response:

Year	Number of Prosecutions
2006	0
2007	0
2008	9
2009	25
2010	16

These responses are current as of 6/14/11

Question Posed by Senator Whitehouse

2. Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Response:

The FBI has recently begun using civil injunctions to combat cyber threats. Historically, the FBI has used solely criminal tools, which have been only partially effective because there are gaps in the forfeiture authorities available to address cybercrime; forfeiture and seizure tools provide limited functionality in this context; and subjects are often able to respond rapidly to our law enforcement efforts and avoid criminal consequences. While we continue to work to address the gaps in forfeiture authority for these crimes, the FBI's efforts to combat complex cyber crimes now benefit from the added flexibility afforded by civil tools. For example, temporary restraining orders and injunctions allow the FBI temporarily to operate computer servers involved in criminal cyber fraud, permitting us to disrupt and dismantle cyber security threats while preventing further victimization.

The recent investigation of the Coreflood botnet in Connecticut is an example of the benefits of supplementing criminal enforcement efforts with civil injunctions. In this instance, the FBI obtained multiple criminal seizure warrants, authorizing us to deactivate the existing Coreflood command and control servers. Simultaneously, we obtained a temporary restraining order that directed the defendants to stop engaging in fraud. The order also authorized the U.S. Marshals Service to respond to infected computers with "stop" commands and to use a substitute command and control server. This approach allowed the FBI to identify many of the victims and notify them of the fraudulent activity and their roles in the scheme. While the botnet was held static, anti-virus vendors were able to develop solutions for detecting and removing the Coreflood virus before a new variant could be released. When the substitute server was activated, it recorded approximately 2.4 million beacons from infected computers; after taking remediation action, the beacons received by the substitute command and control server indicated that the size of the Coreflood botnet had been reduced by approximately 80% domestically and 45% internationally. The temporary restraining order also allowed the FBI to work with private industry and our

foreign law enforcement partners to dismantle the Coreflood botnet. This was significantly preferable to using only criminal remedies, which would have allowed us only to seize the Coreflood command and control servers without addressing the underlying compromised computers. Those compromised computers could then have been recaptured by the subjects of the investigation.

Questions Posed by Senator Klobuchar

3. How does the FBI currently work with private sector entities to counter potential cyber threats before they emerge?

Response:

The FBI has developed strong relationships with private industry, establishing highly effective public-private partnerships such as InfraGard. Through InfraGard, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, this initiative has grown to include more than 42,000 members in 86 chapters across the United States. The exchange of knowledge, experience, and resources generated by InfraGard is invaluable and contributes directly to our ability to counter potential cyber threats.

The FBI also partners directly with the Internet Crime Complaint Center (IC3) and the National Cyber Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. The NCFTA, which includes representatives of industry, academia, and the FBI, participates in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. Both of these partnerships are critical in countering potential cyber threats to the nation's infrastructure, and the FBI routinely provides appropriate information to its InfraGard and NCFTA partners.

In addition to partnerships that address a broad range of cyber threats, the FBI also works directly with organizations that target specific types of cyber threats. For example, in order to better protect banks and consumers against online financial fraud, the FBI has partnered with the Financial Services Information

Sharing and Analysis Center (FS-ISAC) to develop a new model for intelligence-driven collaboration between law enforcement and the private sector. This working relationship began when, during the course of our investigations, the FBI recognized threat trends, tactics, and techniques involving Automated Clearing House (ACH) transactions and invited FS-ISAC representatives to receive a full FBI briefing. When the FBI asked the FS-ISAC whether this threat information would allow businesses and consumers to better protect themselves, reduce their vulnerabilities, and mitigate the consequences of these types of fraud, industry representatives advised that the information was pertinent and that a written product would be useful. In an entirely new collaboration model, we created a joint product in which the FBI wrote the first two sections involving the nature of the threat and how to recognize it and the FS-ISAC (working with the National ACH Association) wrote the second two sections regarding industry impact and security recommendations for preventing further fraud. The President of the FS-ISAC has highlighted this product as a successful example of government sector - private sector information sharing.

a. In what areas do you think improved cooperation would be helpful?

Response:

The FBI's ability to prevent and disrupt the cyber threats depends upon our ability to obtain threat information from the private sector, particularly from service providers. This is because service providers are often able to identify and characterize indications of threat activity (*e.g.*, intrusions and other anomalous behavior) before the FBI becomes aware of the activity. As a result, it is vital that we maintain effective information sharing partnerships with private sector entities.

Although important, information sharing between the public and private sectors can be challenging because both see impediments to sharing with the other. For example, private sector victims of cyber events are sometimes hesitant to share proprietary information with law enforcement because they believe the information will be subject to public release pursuant to the Freedom of Information Act (FOIA) and thus will be available to their competitors. This perception persists notwithstanding our assurances that FOIA allows the government to withhold from disclosure six categories of information that was compiled for law enforcement purposes and information provided to the government that is confidential and commercial in nature. In addition to fearing the release of their proprietary information, private sector organizations may be

reluctant to share information regarding cyber intrusions because they believe their customers will fear for the security of their personal information if they learn that the organization has been victimized by a cyber intrusion.

There are also legal obstacles to the government's ability to share threat information with the private sector. For example, when the government obtains threat information through the grand jury process, the restrictions imposed by Rule 6(e) of the Federal Rules of Criminal Procedure may inhibit the disclosure of that information to concerned third parties in the private sector. In addition, the Electronic Communications Privacy Act (ECPA) prohibits wire, Electronic Communication Service (ECS), and Remote Computing Service (RCS) providers from voluntarily disclosing to the government records and other information pertaining to subscribers or customers of such services, including the contents of such communications, except in narrow circumstances. Specifically, disclosure can be made if the contents of the communication "appear to pertain to the commission of a crime" (18 U.S.C. § 2702(b)(7)(A)(ii)), the disclosure is "necessarily incident to . . . the protection of the rights or property of the provider" (18 U.S.C. §§ 2511(2)(a)(I), 2702(b)(5), and 2702(c)(3)), or the provider, in good faith, believes that an emergency involving danger of death or serious injury to any person requires disclosure without delay of information related to the emergency (18 U.S.C. § 2702(c)(4)).

b. What can Congress do to encourage this cooperation?

Response:

Legal clarity regarding the authority to share and to withhold information would create greater certainty and may improve willingness to share information in appropriate cases. For example, although the FBI believes most computer network exploitation (CNE) events will fall within one or more of the circumstances in which ECPA permits voluntary production, ultimately the decision to share this information must be made by the providers, who will be exposed to legal risk if they interpret the exceptions too broadly. In other words, the statute must afford the providers sufficient assurance that they will not incur liability if they share this information with the government. To the extent there is uncertainty whether the ECPA's exceptions apply to a suspected CNE, the statute creates a potential obstacle to the prompt sharing of threat information by ECS and RCS providers. Providers would presumably be more willing to voluntarily give the FBI access to ECPA-protected information where CNE is suspected if there were a clearer carve-out to cover that circumstance.

These responses are current as of 6/14/11

Questions Posed by Senator Hatch

Comprehensive Cyber Doctrine

4. Mr. Snow, I am concerned we do not have a comprehensive doctrine for Cybersecurity. During the Cold War our nation developed doctrines to deter the spread of communism and defined how the United States would react if attacked. Today, our policies are not nearly as clear. In the Cold War, the enemy also understood the theory of mutually assured destruction and strike back capability. However, in the cyber world, an enemy could hinder or eliminate our ability for retaliation in the first wave of a cyber attack. Fundamental questions have yet to be answered.

a. According to the FBI, what constitutes an attack against the United States?

Response:

While the FBI is a key partner in the comprehensive multi-agency response to cyber-based threats to our national security, investigating cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, computer intrusions targeting the national information infrastructure, and other cyber crime, we do not assess whether these intrusions constitute "attacks against the United States."

b. Since the FBI is both a law enforcement agency and a member of the U.S. Intelligence Community, how does the FBI weigh in on these issues?

Response:

In addition to investigating cyber crimes in furtherance of the FBI's law enforcement mission, the FBI's Cyber Division includes sections that focus specifically on matters related to our role in the U.S. Intelligence Community (USIC). For example, the Cyber Intelligence Section provides actionable intelligence in support of the Cyber Division's intelligence functions, while the Cyber National Security Section provides program management related to counterterrorism and counterintelligence computer intrusions. The FBI works through the Department of Justice and the Office of the Director of National

Intelligence (ODNI) to raise concerns and address policy matters related to both our law enforcement and intelligence roles.

c. How is intelligence information pushed up the line to policy makers and decision makers regarding attribution and identifying those responsible for the attack?

Response:

FBI intelligence is disseminated formally through standard USIC products (including Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments) and is routinely incorporated into multi-agency products (including ODNI/National Intelligence Council products). In addition, the FBI works with the National Cyber Investigative Joint Task Force (NCIJTF) to develop tactical operational plans targeting those responsible for attacks, providing those plans to senior policy makers for review and approval. The FBI also routinely provides briefings to policy and decision makers within the Executive Branch, Congress, and the private sector.

National Cyber Investigative Joint Task Force

5. Hackers can simultaneously attack our critical infrastructure. These hacks impact banking systems, electrical grids, transportation systems and military networks. However, based on our organizational structure, the responsibility for defending these systems falls to a variety of different agencies. This could give the hacker an advantage unless information is shared. I am aware that the FBI leads the National Cyber Investigative Joint Task Force. This national center has personnel from a variety of agencies and entities assigned there, including the Secret Service. What is the dynamic inside the task force? Are agencies cooperating with one another?

Response:

The NCIJTF is a collaborative organization in which all participants are aware that cooperation is the key to success and are dedicated to ensuring that success. This task force enables the U.S. Government to execute a coordinated response to cyber threats by using domestic law enforcement and foreign intelligence authorities together in concert, coordinating and integrating the counterterrorism, counterintelligence, intelligence, and law enforcement activities of task force members. Although most of those who make up the NCIJTF are full-time task force members, some agencies are unable to dedicate a full-time cadre and instead

have their members attend only those meetings focused on threat topics of particular interest to that agency.

Because the task force's organization is designed to foster collaboration, its structure encourages the discovery of related intelligence and investigative targets, strengthened situational awareness of threat actors and motives, and faster and more reliable execution of intelligence and investigative objectives (such as determining threat attribution). The NCIJTF also facilitates the deconfliction of agencies' activities and the reconciliation of competing equities at a tactical level, often leading to more cooperative and mutually beneficial outcomes.

Challenges are inherent in the combination of agencies with different missions, authorities, focuses, and resources. Nonetheless, the close working environment and collaborative approach have been extremely successful, with significant work among key national cyber investigative and intelligence contributors leading to better awareness of the needs and goals of counterparts at other agencies and facilitating collaboration in circumstances where it might not otherwise have occurred. Many member agencies now find the NCIJTF an indispensable enabler of their own investigative or intelligence missions.

The NCIJTF's accomplishments have been acknowledged by the USIC. In August 2009, in recognition of the exceptional service of the NCIJTF's alliance of peers, operators, and analysts, who worked together on threats of concern from April 2007 to April 2009, the ODNI presented to the NCIJTF a National Intelligence Meritorious Award. The award acknowledged that the NCIJTF "was the driving force behind the transformation of cyber threats from a fragmented and reactive individual agency response, to a unified and highly successful proactive national effort that established itself as a national center of excellence."

Before the United States Senate Judiciary Committee, Subcommittee on Crime and Terrorism
"Cyber Security: Responding to the Threat of Cyber Crime and Terrorism"
April 12, 2011

Responses to Questions Submitted by Senator Orin Hatch
By John E. Savage

International Cooperation

Professor Savage, in your prepared statement you advocate for exploring proposals for effective international cooperation on the development of cyberspace norms and rules of the road. I believe that a strong cyber policy should be a topic of discussion in trade agreements and included in economic and foreign policy strategies when we engage foreign nations in diplomacy.

1. **In order to gain effective international cooperation, do you believe that enforcement of the rule of law in cyber crime should be included into trade agreements?**

Because I have only a general layperson's knowledge of trade agreements, I do not have an expert opinion on the role that the rule of law on cyber crime should have in such agreements. However, I am sufficiently knowledgeable about the Council of Europe Convention on Cybercrime (CoC) to appreciate that it can help to understand the value and efficacy of treaties that do require adherence to the rule of law on cyber crime.

The CoC advertises itself as "the only binding international instrument dealing with cybercrime." It is designed to a) harmonize national laws on cybercrime, b) improve national capabilities to investigate such crime, and c) enhance international cooperation in this area.

Its effectiveness may be judged by the fact as of April 25, 2011, 30 countries have ratified the convention. While my personal knowledge of the effectiveness of CoC is limited, the experience of federal law enforcement agencies with the agreement is informative. Deputy Assistant Attorney General Jason Weinstein, a member of the first panel, testified that the Department of Justice relies on the CoC "to provide a framework for efficient cooperation among nations involving electronic crime."

I take this as a strong endorsement of the effectiveness of insisting on enforcement of the rule of law concerning cyber crime when developing international agreements.

2. **Any thoughts on how best we can determine which countries are countries of concern?**

During my year in the U.S. Department of State as a Jefferson Science Fellow I learned that the U.S. government makes assessments of which countries are of concern in the cyber arena. This information should be available to the committee in the appropriate forum.

It is often said that a very large fraction of the information that forms the basis for intelligence assessments is available in the general press. Thus, major news outlets, such as the Washington Post, the New York Times, and Reuters, can provide reports that can help to identify countries of concern. A recent Reuters article[1], which

[1] Special Report:In cyberspy vs. cyberspy, China has the edge,Reuters,April 14, 2011.

quotes many authoritative American sources, argues that China is a major threat to the U.S.. Reports of the U.S.-China Economic and Security Review Commission also speak to this issue.

International Definition of Cybersecurity in International Law

Professor Savage, our nation, has a unique opportunity to take a strong leadership role in defining Cybersecurity in international law. I concur with the sentiments of your statement the United States should promote the acceptance of Cybersecurity legal definitions and rules of the game. These should be beneficial to the United States and promote international cooperation.

1. **What international body or convention do you believe should be the guardian of Cybersecurity agreements and definitions at the international level?**

At the moment there is no one international body or convention that is an acceptable guardian of cybersecurity agreements and definitions. Some members of the International Telecommuncation Union (ITU) would like it to play that role, although many in the U.S. are opposed to that proposition. Observing this landscape, the authors of two recent reports described below, while expressing serious reservations about the ITU, nonetheless express alarm that the U.S. is not adequately engaged in international discussions of cybersecurity and Internet governance.

In a September 2010 report[2] for the Council on Foreign Relations, Robert Knake wrote that, because we have not been fully engaged, the U.S. is being outmaneuvered in those international forums that determine the future of the Internet by countries who favor state control of the Internet. He says that the best way to encompass all the issues and the players involved in cyber security is to "nurture a range of forums – some multilateral, some bilateral, and some regional – to tackle these challenges." This would avoid state-centered control of the Internet, which he finds unsatisfactory and characteristic of the ITU. He cites the Financial Action Task Force established in 1989 by the G7 as an example of an international body that might be emulated.

In a recent article[3] Sofaer, Clarke and Diffie echo the urgent need for the U.S. to engage other nations in negotiating international agreements. They describe three general preparatory steps that have been effective in striking agreements in the past. They are to a) determine the topics that a nation wants included and excluded from agreements; b) define the measures it wishes be incorporated into agreements, such as declarations, information sharing, prohibitions, punishments, cooperation, and standards and practices; and c) the types of administrative structure and allocations of authority that it would like to see in agreements. For each step they describe the issues that they believe are important to the U.S. They close by acknowledging the difficulties and uncertainties involved in striking international agreements.

Before engaging in international cybersecurity agreements, the U.S. government must develop a coherent national cybersecurity strategy, which it should do in conjunction with the public and private sectors.

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I've been following this issue very closely and would appreciate learning your views on some the legislative proposals that are pending?

---

[2] Internet Governance in an Age of Cyber Insecurity, Robert Knake, Report No. 56, Council on Foreign Relations, September, 2010.

[3] *Cyber Security and International Agreements*, Sofaer, Clark and Diffie, **Procs. Workshop on Deterring CyberAttacks**, National Academies, Press. 2010.

1. What are some of the issues we should avoid and others we should embrace?

S. 773, the Cybersecurity Act of 2010, introduced in the 111th Congress, is an excellent bill. It highlights the need to identify critical infrastructure sectors of the U.S. economy, outlines steps to develop a cyber aware and educated workforce, defines the cybersecurity responsibilities of the executive branch in both domestic and international arenas, highlights the need to educate the general public as well as university students, identifies areas for public-private collaboration, provides funding for research in critical cybersecurity areas and calls for the incorporation of cybersecurity into the curricula for industrial control system engineers.

The bill also speaks to the need to certify and accredit cybersecurity degree programs. Unfortunately, it is too early to do that. Top computer science departments typically offer zero or one course on computer security and possibly one or two courses on cryptography. Thus, universities need to be encouraged to introduce cybersecurity course sequences in computer science departments, not just in industrial control curricula.

An attractive feature of S. 3155, the International Cybercrime Reporting and Cooperation Act, introduced in the 111th Congress is the requirement that assistance be provided to UN nations that have a low level of development or utilization of information and communications technologies in key industries. That type of support will win over developing nations whose support we need in the ITU. The bill also would require the President to provide help to "countries of concern" to improve their capacity to combat cybercrime. While laudable, I doubt that such countries will want to cooperate after being identified as a country of concern. It would be better to fund studies in the U.S. on steps that might be taken to encourage the desired behavior. A good example of a productive move that should be further encouraged is the set of talks sponsored jointly by the U.S. Center for Strategic and International Studies (CSIS) and the China Institutes of Contemporary International Relations (CICIR). My understanding is that these talks have brought together private and governmental U.S. representatives to meet with their Chinese counterparts. This form of informal diplomacy may prove to be very productive.

S. 413, the Cybersecurity and Internet Freedom Act of 2011, introduced in the 112th Congress would create the Office of Cyberspace Policy in the Executive Office of the President. The U.S. very much needs to develop a national cybersecurity strategy. This bill imposes a large range of demanding responsibilities on the office and probably will require a large staff. If the new office is to replace the Cybersecurity Coordinator's Office (approximately seven staff), it is not likely that it can satisfy its mandate.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime &Terrorism
April 12, 2011

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I've been following this issue very closely and would appreciate learning your views on some the legislative proposal that are pending? What are some of the issues we should avoid and others we should embrace?

Phyllis Schneck Response:

Issue Summary: The cyber security threat landscape has changed fundamentally over the last decade. According to the Center for Strategic and International Studies, crime syndicates, terrorists, and nation states are engaging in cyber attacks to steal billions of dollars in intellectual property, disrupt businesses, and threaten governments. These sophisticated actors are capable of damaging or shutting down vital parts of the global economy. And the threat to national governments and critical infrastructures has never been greater. In response, policy makers are now engaged in a once in a decade revision of the nation's cyber security laws. They are considering a wide range of options that include updating rules governing the way Federal agencies manage cyber security, requiring critical infrastructure industries to upgrade their security regimes, creating a national, uniform system of breach notification, and increasing investments in university cyber security research and training.

McAfee Priorities:

Presidential Leadership: To date, no single individual or entity has been given the responsibility to coordinate all of the Federal government's cyber-security related activities. This has resulted in a patch-work of cyber security programs, some effective, and others less effective. We support the President's appointment of a Cyber Czar. For the Cyber Chief to be as successful as possible, he/she needs to be given direct access to the President and genuine authority or leverage over agency budgets. We likewise support legislation that would mandate the appointment of a Cyber Czar that reports to the President.

Agency Leadership: Holding the leadership of Cabinet Departments and independent agencies accountable for information security management is a vital objective. Each agency should have a Chief Information Security Officer (CISO) who has the authority and budget to continually upgrade security processes, technologies, and people to ensure that agency is sufficiently protected. Each agency CISO should be aligned with colleagues in the agencies and in the private sector to gain visibility into cyber events and trends, and have the capability to immediately take joint action in crisis situations. Each CISO should have a trusted public-private collaboration team assembled long before a crisis.

Agencies with cyber leadership responsibilities should be provided adequate funding to assemble "A players" in technology, and policy for rapid and effective execution. Leadership should be empowered to incentivize top talent and release resources that are not effective, removing political obstacles from needed progress, and making government work more attractive to the best minds in the nation.

FISMA: We have long supported the *Federal Information Security Management Act* (FISMA) process and believe that most agencies are doing their best to comply with the law. However, while FISMA compliance grades may have improved over the years, there appears to be a limited correlation between an agency's FISMA compliance and the state of its cyber security posture. We thus support Federal legislation to transform FISMA into an operational frame work that will help agencies produce continuous system and

process improvements that can be quantified and verified. Toward this end, agencies should be required to do an annual gap analysis that identifies deficiencies and provides program objectives and milestone plans to close these gaps. These reports should also address agency needs for additional resources and funding to ensure these gaps are closed. The executive branch should likewise continue to roll out its continuous monitoring model of information gathering that is effectively replacing paper reports as a means of delivering performance metrics.

Breach Notification: Forty-four states enforce breach notification laws. While these laws play a vital role in pushing organizations to improve their data management rules and processes, this system of state laws is inefficient and makes compliance difficult given their lack of uniformity. Congress should pass a uniform breach notification law. Such action would send a clear signal to the market on the need to improve data security practices, while also making compliance and enforcement predictable and efficient. Legislators should consider the merits of modeling their breach notification proposals on the rules that are already in place for medical information mandated by the Health Information Technology for Economic and Clinical Health Act or HITECH Act.

Standards: The global IT industry is fast moving and depends on rapid innovation to meet customer requirements. The government should defer to de-facto standards or to private sector standards setting bodies to ensure that IT companies can continue to develop products that meet the needs of global customers. Industry activities to rationalize assurance standards should also be supported by the government.

Any standards developed by the US government should be done in consultation with the private sector and should specify process, performance criteria or functional specifications, not specific products or technologies without duplication. NIST should collaborate with other government agencies that have unique expertise in cyber security (the Energy Department's expertise, for instance, in addressing electric and nuclear cyber-vulnerabilities) and take the lead in coordinating the Federal government's agenda in the development of international cyber security standards. Standards advocated by the US Government should be consistent with standards recognized by such international bodies as ISO.

Special attention should be paid to what has led to success in more narrowly defined arenas. For example, the Department of Defense and the National Security Agency have developed a seven-zone defense in depth security architecture with mandated functional protections in each area. At a minimum, US Federal Civilian agencies and Defense Industrial Base entities should be mandated to use the same standards. The Department of Homeland Security and DC3 should be charged with managing compliance audits and enforcement of these standards.

Public/Private Partnership on Information Sharing and Information Exchanges: To further promote public/private partnerships, existing government bodies should be leveraged in a more streamlined way. The Enduring Security Framework, a body to which McAfee belongs, is a success and should be used as best practice model. The public/private partnerships managed by the Department of Homeland Security should be streamlined and up-leveled to ensure that senior corporate officials and senior government officials are positioned to share vital information and best practices. Furthermore, too often the current legal system acts as a disincentive for productive information sharing. Liability reforms need to be enacted to help incent companies to share vital information on cyber security threats with their government counterparts.

Department of Homeland Security Einstein 3: Commercial off the shelf technologies (COTs) have proven their ability to protect the most sensitive government sites and IT systems. For instance, COTs is the basis of Department of Defense's Host Based Security System, one of the most successful cyber security implementations in the Federal government. Einstein 1 and 2 have been based on a proprietary technology sponsored by the government, and these programs have consistently failed to meet expectations. Einstein 3 should include COTs solutions, and they should be mixed and matched with government proprietary technologies as appropriate to enable the Department of Homeland Security to roll out a world-class cyber security program.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime &Terrorism
April 12, 2011

(Weinstein) Definition of Cybersecurity In International Law
Mr. Weinstein, our nation has a unique opportunity to take a strong leadership role in defining Cybersecurity in international law. What are the steps that the Justice Department is taking to define Cybersecurity in international law?

Answer:

The Department of Justice agrees that the United States should take a leadership role in forging consensus regarding international law as it pertains to cyberspace. Building on existing norms, legal principles, international agreements, and domestic law, we believe that the United States has an opportunity to build shared understandings regarding international law as it pertains to cyberspace in a positive way that fosters innovation, promotes freedom of expression, and prohibits malicious cyber activity. As discussed below, numerous elements of the United States Government have important roles to play in the development of international cyber law.

Cybersecurity (a subcategory of international cyber law) is a broad concept that encompasses many disciplines and agencies of the United States Government. The Department of Justice is an important component in protecting our nation's cybersecurity, but our efforts in this area involve collaboration with the Departments of Homeland Security, Defense, State, Commerce, and several others.

The Department is working with our interagency partners to lead and develop international consensus in each aspect of cybersecurity.

To carry out the Department's primary responsibility, the promotion of effective investigations and prosecutions of cyber-offenders, the Department continues to take a leadership role in promoting the Budapest Convention (Council of Europe Convention on Cybercrime), which the Department helped negotiate and worked with the Senate to ratify in 2007. The Convention pioneered the international definition of key cybercrimes and the tools necessary to investigate crimes committed using computers and networks.

The Department continues to work with our international partners to build their law enforcement and prosecution capacities. We use State Department Foreign Assistance funds to provide capacity-building training and technical assistance to developing countries, including advice on developing their legal frameworks in this area.

Due to the transnational nature of most cybersecurity incidents, achieving effective multilateral cooperation in real time has become a priority. The Department actively promotes tools for international law enforcement cooperation and information sharing, such as the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid

law enforcement coordination across borders.

Senator Sheldon Whitehouse
U.S. Senate Judiciary Committee
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime &Terrorism
April 12, 2011

Question to Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice; Gordon Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation; and Pablo Martinez, Deputy Special Agent In Charge, Criminal Investigation Division, Cyber Crime Operations, United States Secret Service. Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Answer:

Given the increasingly complex threats we face, the Department uses both civil and criminal authorities to counteract a variety of online crimes. Most recently, on April 13, 2011, the Department combined civil and criminal statutory authorities in an effort to disable the Coreflood botnet in the most comprehensive enforcement actions ever taken by U.S authorities against an international botnet. The operators of the botnet surreptitiously spread malicious software to hundreds of thousands of computers across the United States. Among the functions of the botnet was code that silently captured private communications and financial information of victims. In that case, the Department announced the filing of a civil complaint, the execution of criminal seizure warrants, the issuance of civil forfeiture seizure orders for domain names, and the issuance of a temporary restraining order and later a preliminary injunction. The U.S. Attorney's Office in Connecticut filed the civil complaint against 13 John Doe defendants, alleging that the defendants engaged in wire fraud, bank fraud, and illegal interception of electronic communications. In addition, search warrants were obtained for computer servers throughout the country, and civil seizure warrants were obtained in the U.S. District Court for the District of Connecticut for 29 domain names. Finally, the government obtained a temporary restraining order, authorizing the government to respond to signals sent from infected computers in the United States in order to stop the Coreflood software from running. This action prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the United States. This action was taken in close consultation with computer security and industry experts.

The Department will continue to be creative and aggressive in using appropriate and lawful tools – both civil and criminal – to bring down botnets and other forms of serious international cyber crime.

SUBMISSIONS FOR THE RECORD

"Cyber Security: Responding to the Threat of Cyber Crime and Terrorism"

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security

Before the Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

April 12,2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and members of the subcommittee. My name is Stewart Baker. I have been involved in cybersecurity issues since the early 1990s, when I was General Counsel of the National Security Agency, and most recently as Assistant Secretary for Policy at the Department of Homeland Security during from 2005 to 2009. I appreciate the opportunity to address this vitally important issue.

Everyone knows that cybercrime is a problem. But everyone also seems to believe that the problem can be solved with modest additional effort.

In fact, cybercrime -- and the vulnerabilities on which it feeds -- will soon pose a profound challenge to our way of life, and perhaps even to America's role in the world.

Those who think the problem of cybercrime can be easily solved have embraced little myths that help them avoid taking harder steps.

I'd like to begin by identifying those myths and debunking them, because we won't begin to address the problem until we recognize that the easy solutions will not work. (I discussed several of these myths in my book, *Skating on Stilts*, and I've drawn on that material for today's testimony.)

Law Enforcement in Cyberspace: Not Even a Myth

Before I do, though, I'd like to address one solution that isn't taken seriously enough to even qualify as a myth: the notion that law enforcement can solve the cybercrime problem. It is true that federal authorities occasionally catch and prosecute a successful hacker. But those successes are dwarfed by the massive number of uncaught, unprosecuted, and even unreported hacks that occur every day. Very few victims even bother to go to the authorities any more. It would be like complaining that someone stole a wallet from your unlocked car in a bad neighborhood. You know, and so do the authorities, that the chances of solving the crime are so remote that even going through the motions of a report and investigation isn't worth the trouble.

Most problems of social disorder are contained by the threat of punishment. Human society depends so profoundly on social punishment as a survival mechanism that it is built into our genes. We have reward centers in our brains that fire when we punish rule-breakers – even if we can expect no individual benefit from a change in the rule-breaker's future behavior. Many of us will even incur costs just to punish rule-breakers we will never see again. (I probably don't have to tell you that if you've ever driven in Washington traffic.)

Yet the ease with which attackers can hide in cyberspace makes it almost impossible to punish criminal conduct online. We simply cannot identify the criminals. And so we find ourselves trying to build an online society where there is no real punishment for lawless behavior. Whether this is even possible is open to question. Those who think it is possible are counting on computer security – a bombproof defense – to make up for our inability to punish wrongdoers.

Counting on a bombproof defense would be a dubious proposal in the best of circumstances. It is particularly dubious when one realizes just how much of our defense is built on myths rather than reality.

The Myths That Keep Us from Dealing Squarely with the Cybersecurity Crisis

Myth 1: It's a Microsoft Problem. I know plenty of people who still believe that Microsoft's products are uniquely insecure, and that we could solve the problem if we could just get Microsoft to clean up its act. For some, the security of Linux was an article of faith; its source code is open to inspection by anyone, so it is protected from exploit by all those watching eyes. And Apple, which didn't even offer an antivirus program for decades, was protected by Steve Jobs's sheer coolness.

The last few years have been hard on those illusions. As Apple gained market share, malware authors began writing for its operating system, and they didn't have any trouble finding holes. And all those eyes on Linux's code? In August of 2009, two Google researchers discovered a bug in the central core of Linux; it would allow an attacker to acquire complete administrative control of any machine to which he had physical access. You might call that a success for open source, except that the bug had been hiding in plain sight for at least eight years.

Why, then, is there so much more malware running on Windows than on Linux? Almost certainly for the same reason that there are more applications of every sort running on Windows than on Linux. Like other application developers, malware authors want to reach the largest number of users with one piece of code. And the way to do that is to write your application for Windows.

Myth 2: It's a Password Problem. It's an article of faith among the security-conscious that passwords are a big security hole. People can't remember the hard ones, and hackers have assembled dictionaries of all the memorable ones. Plus, it's easy for hackers with access to a machine to capture the user's keystrokes as he types his password in.

So for real security, companies and government rely on tokens. RSA makes a common token. Every thirty seconds it displays a different security code, known only to the user and his network server. Even if a hacker could compromise my machine and record all my keystrokes, he couldn't know what the token was going to say thirty seconds from now. But hackers have demonstrated in two ways that tokens of this kind are no long-term solution. First, RSA recently announced that hackers had broken into RSA's network and compromised the security of the system. RSA is not providing a lot of details to the public, but it seems quite possible that, at least for some tokens, the hackers can now predict exactly what the token will say every thirty seconds, for years to come. And even those who cannot predict the token's future code have found a way to beat these token systems. Now, when the owner of a compromised machine starts typing in his temporary code, the malware immediately sends a real-time message to its sponsoring hacker. As the owner types, each digit is sent to the hacker, who simply logs in right along with the owner.

Myth 3: Really Important Transactions Can Be Confirmed Offline. More sophisticated users know that their home machines simply cannot be trusted. To protect their financial accounts, they've locked them up; they may bank on line, but no serious money can leave their account unless the bank calls to verify the transaction.

In fact, even those who haven't locked everything down may get a verifying call. Like the credit card companies, mutual funds and financial institutions have stopped trusting their customers' computers. For risky transactions, they insist on offline, or out-of-band, confirmation.

Out-of-band communication is today's most common fail-safe solution for computer compromises. But using another line of communication won't solve the problem for long. Finding a truly offline method of communication is going to get harder. Businesses and consumers are switching in large numbers to "voice over IP," or VoIP, telephony. They cannot resist the allure of bringing to voice communications the cheap, flexible features of Internet communications. But the switch means that they are also bringing to voice communications all the insecurity that plagues other Internet communications. In fact, telephone insecurity could be worse, as users download apps from unknown providers to no-name phones made cheap in the People's Republic of China, where hacking remains widespread. If an attacker who has compromised your computer's online bank account is also able to divert calls to your Internet telephone, then it will be easy for the attacker to confirm that you really do want to transfer your life savings to Moldova or Nigeria.

Myth 4: If Worse Comes to Worst, We'll Disconnect Our Critical Systems from the Internet. The government used to have its own special illusion about security. Maybe our unclassified networks are compromised, Defense Department officials would say, but the classified networks are still bombproof. They can't be compromised because they aren't connected to the Internet. There's an "air gap" between the two. That assumes, of course, that network security decrees are perfectly enforced—and that the most important secrets are only discussed on classified networks—notions that contradict everything we know about human nature. But never mind, because the air gap illusion, too, has fallen prey to the exponential empowerment of hackers that we've seen in recent years.

The French navy's Rafale Marine jets train out of Villacoublay air base, in the southwest suburbs of Paris. These fighters are state of the art, packed with stealth and electronic warfare capabilities and capable of landing on carriers. But to do that, they first have to take off. And for two days in January 2009, the jets couldn't take off.

They'd been grounded by a hacker.

The "Conficker" computer worm had been exploiting vulnerabilities in Windows servers for months. It was the most ambitious computer infection in years. At the time it had infiltrated as many as 15 million machines around the world. One of the ways it spreads is by infecting the USB thumb drives that carry data from one machine to the next. Even classified or isolated networks could be captured if a bad thumb drive was used to transfer data to a machine on a secured network.

That's what grounded the French fighters. Before the navy even knew it was under attack, the worm was coursing through its internal network. Rushing to contain the damage, the navy told its staff not to turn on their machines, and its systems administrators began quarantining parts of the network.

Too late for Villacoublay. Its systems were already hosed.

The Rafale fighter downloads its flight plans, a far more efficient process than paper-based systems. But once the contagion had spread to Villacoublay no flight plans could be downloaded. Until an alternative method of delivering the flight plans could be cobbled together, the Rafales were no more useful than scrap iron. The French press reported the embarrassment in detail.

Perhaps as consolation, the papers were careful to note that things could have been worse—and were, in Great Britain. There, the French press said, twenty-four Royal Air Force bases and three-quarters of the Royal Navy Fleet had succumbed to Conficker. The British and French navies may have been unintended victims of a worm designed for criminal ends. But after Conficker, no one can believe that an air gap is a security fail-safe.

Indeed, the Deputy Secretary of Defense has acknowledged that hackers successfully jumped the air gap to compromise DOD's classified networks. And it is hard to believe that the Iranian government did not keep its Natanz enrichment plan far from the Internet – a tactic that evidently did not prevent the Stuxnet malware from making the jump via thumb drive.

Myth 5: They're Not Looking for Me. The last of our illusions is that we're just not that interesting. Other people have more money. Other people have more valuable secrets. Who's going to come looking for me?

That's the last hope of every herd animal. The predators can't eat everyone. If you lie low and blend in, they won't pick you.

Wrong on two counts, I'm afraid. First, take this test. Add up your savings, car value, house equity, and investments. Is the total over $65,000? If so, you've got a lot of company on the

globe. Probably 10 percent of the world's 6.8 billion people have assets exceeding that amount—say 700 million in all. Being one in 700 million sounds like pretty good herd-animal odds until you realize that, for every person with more than $65,000, there are nine people with less. As computers become exponentially cheaper, most of those nine people will be able to get online. Then there will be nine people to see you as a rich outsider who deserves to be relieved of his assets. And another nine for your spouse, nine for your neighbor, and nine for each of your business partners. Maybe nine each for every person you know.

The world is already full of scam artists willing to work for less than minimum wage. Most of them know English and have access to the Internet. The relentless march of empowerment will soon give those scam artists new tools for finding and fleecing you.

They can send out ten million emails telling people that they've won the Spanish lottery. If one in ten thousand responds, even with great caution, that person has selected himself for fleecing, and the pitch can then be tailored precisely to his failings.

So what if that part of the scam is a bit labor intensive? There are as many as nine people with nothing better to do than sit around trying to get into the mark's head.

In fact, it's worse than that. Because Moore's Law is working for the outlaws too. The increasing speed of new computers means that outlaws can use the victim's own computer to decide whether he's interesting enough to rob.

Remember that real-time password-stealing program? Well, the thieves don't have to go looking for rich people to infect. Instead, they infect everyone, and let the malware find the rich ones. The password-stealing program consumes an infinitesimal part of a modern chip's processing power to run quietly in the background, watching and waiting until its victim logs on to one of about fifteen hundred predetermined financial sites. Anyone logging in to one of those sites, the authors figure, probably has enough money to be worth cleaning out.

So when an infected computer sets itself apart from the crowd by logging on to a financial site, the malware alerts its author, who can now focus on taking money from that computer's owner. Moore's Law has taken a lot of the work out of the hunt. And, thanks to the empowerment of information technology, it will keep making the job exponentially easier, year in and year out.

What Can We Do About Cybercrime?

In short, cybercrime is bad now, but it will be far worse in the future. The success of cybercriminals has already inspired more than a dozen governments to flirt with cyberweapons. And Stuxnet shows that some have moved beyond flirtation.

Stuxnet seems to have been highly targeted on the industrial control system for centrifuges in a single facility in Iran. But the tools it deployed could just as easily be used to bring down the power grid for a city or a region – and probably also to destroy the generating equipment on which the region depends, forcing city dwellers to live without power for weeks or months, if they can.

That kind of attack would change the nation. The leaders who failed to prevent the attack would be swept away, and massive changes would be made in our information networks to thwart future attacks.

Or perhaps we'll escape an international conflict. Even if we are that lucky, cybercrime will keep growing, for all the reasons I've already given. It is dead easy, and it pays remarkably well. We shouldn't wait for disaster if we can head it off.

The problem is that any change big enough to seriously address the problem is big enough to offend one or more well-represented lobby. With that in mind, and with some diffidence, let me sketch the kinds of changes that might change the direction in which we are traveling.

First, when you can't trust the devices on your network, which is increasingly true of all organizations, one successful defense seems to be back-office pattern recognition. The most obvious use of this technique is the system that credit card companies use to stop suspicious transactions; anyone who has used a credit card in an unusual context is familiar with the "just checking" calls that come from the card issuer. We need to create incentives for companies to deploy such systems more widely. Two examples: US home computers are badly infected and widely used for bot attacks and other crime. The ISPs that carry traffic from these infected machines can often identify the machines from their pattern of behavior. But the ISPs have no incentive, and much disincentive, to notify the owners, or to quarantine or restrict the machine's access to the internet. Similarly, small businesses that have been compromised with key loggers cannot protect their Electronic Funds Transfer accounts from hackers on their own. The banks that receive unusual EFT requests are in a much better position to spot a fraud in the making, but today liability for that fraud rests on the business owner, not the bank. Again, finding a way to encourage banks to use their central position in the payment stream to identify EFT fraud would likely make fraud less attractive.

Another way to reduce cybercrime is to reduce anonymity in cyberspace. Better attribution of machines and users on networks will make it easier to punish lawbreakers, and without punishment of those who break the law, all the defenses in the world are not likely to succeed.

There are no doubt other steps that could be taken, but at this point, the federal government doesn't even have authority to call on industry to take obviously needed security measures. The Defense Department lacks insight into the origins of critical supply-chain components. The federal government lacks authority to set high security standards for the industries on which our civilization depends. Congress has been considering bills to address these security gaps for many months; it's past time to enact one.

Finally, deep as this security hole is, we should at least stop digging. We should slow or stop initiatives that will increase our risk. The "smart grid" movement, for example, won't look so smart if it results in a whole new set of vulnerabilities for the populace as a whole; we need confidence in the entire security architecture before we deploy smart grid technology. By the same token, filling our telecommunications networks with unvetted equipment from vendors

beholden to the Chinese government makes little sense, yet the administration apparently felt compelled to approve foreign vendors as the beneficiaries of federal broadband stimulus funds.

I offer these ideas not because they will all work or they are all the best possible solution but to show the kinds of changes that we must be willing to consider if we want to bend our extraordinarily risky trajectory. But if you kept track of the industries, the foreign governments, and the civil liberties groups likely to be offended just by that short list of possible measures, you understand why we are still sliding down a slope that leads to serious trouble.

Thank you for your attention.

White Paper

McAfee

Global Energy Cyberattacks: "Night Dragon"

By McAfee® Foundstone® Professional Services and McAfee Labs™

February 10, 2011

Table of Contents

Executive Summary

In 2010, we entered a new decade in the world of cybersecurity. The prior decade was stained with immaturity, reactive technical solutions, and a lack of security sophistication that promoted critical outbreaks, such as Code Red, Nimda, Blaster, Sasser, SQL Slammer, Conficker, and myDoom—to name a few. The security community has evolved and grown smarter about security, safe computing, and system hardening but so have our adversaries. This decade is setting up to be the exponential jumping off point. The adversaries are rapidly leveraging productized malware toolkits that let them develop more malware than in all prior years combined, and they have matured from the prior decade to release the most insidious and persistent cyberthreats ever known.

The Google hacks ("Operation Aurora"), named by McAfee and announced in January 2010, and the WikiLeaks document disclosures of 2010 have highlighted the fact that external and internal threats are nearly impossible to prevent. Miscreants continue to infiltrate networks and exfiltrate sensitive and proprietary data upon which the world's economies depend every day. When a new attack emerges, security vendors cannot stand by idly and watch. We are obligated to share our findings to protect those not yet impacted and to repair those who have been. As such, McAfee Foundstone Professional Services and McAfee Labs decided to release the following discovery.

Starting in November 2009, coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. We have identified the tools, techniques, and network activities used in these continuing attacks—which we have dubbed Night Dragon—as originating primarily in China. Through coordinated analysis of the related events and tools used, McAfee has determined identifying features to assist companies with detection and investigation. While we believe many actors have participated in these attacks, we have been able to identify one individual who has provided the crucial C&C infrastructure to the attackers. *(See Appendix B for more detail on attribution.)*

Anatomy of a Hack

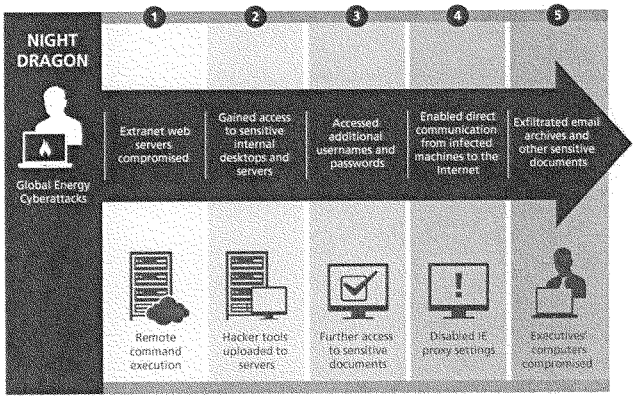


Figure 1. Anatomy of a hack.

The Night Dragon attacks work by methodical and progressive intrusions into the targeted infrastructure. The following basic activities were performed by the Night Dragon operation:

- Company extranet web servers compromised through SQL-injection techniques, allowing remote command execution
- Commonly available hacker tools are uploaded on compromised web servers, allowing attackers to pivot into the company's intranet and giving them access to sensitive desktops and servers internally
- Using password cracking and pass-the-hash tools, attackers gain additional usernames and passwords, allowing them to obtain further authenticated access to sensitive internal desktops and servers
- Initially using the company's compromised web servers as command and control (C&C) servers, the attackers discovered that they needed only to disable Microsoft Internet Explorer (IE) proxy settings to allow direct communication from infected machines to the Internet
- Using the RAT malware, they proceeded to connect to other machines (targeting executives) and exfiltrating email archives and other sensitive documents

Details of the Attack

Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information. The primary operational technique used by the attackers comprised a variety of hacker tools, including privately developed and customized RAT tools that provided complete remote administration capabilities to the attacker. RATs provide functions similar to Citrix or Microsoft Windows Terminal Services, allowing a remote individual to completely control the affected system.

To deploy these tools, attackers first compromised perimeter security controls, through SQL-injection exploits of extranet web servers, as well as targeted spear-phishing attacks of mobile worker laptops, and compromising corporate VPN accounts to penetrate the targeted company's defensive architectures (DMZs and firewalls) and conduct reconnaissance of targeted companies' networked computers.

SQL Injection Attacks

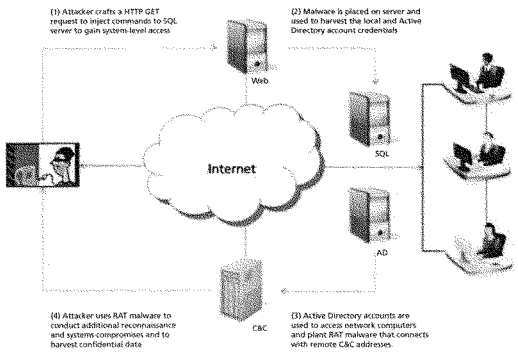


Figure 2. SQL-injection attacks.

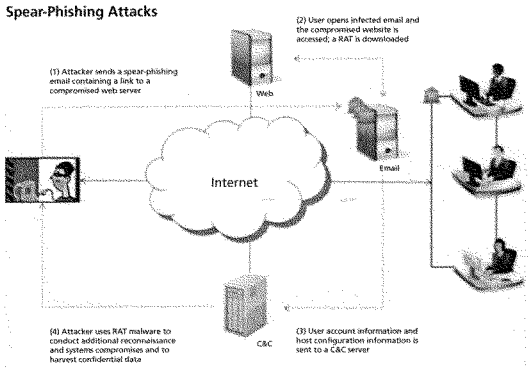


Figure 3. Spear-phishing attacks.

Many Chinese hacker websites offer these tools for download, including links to reduh, WebShell, ASPXSpy, and many others, plus exploits and zero-day malware.

Figure 4. Rootkin.net.cn offers access to an endless list of hacker tools and exploits.

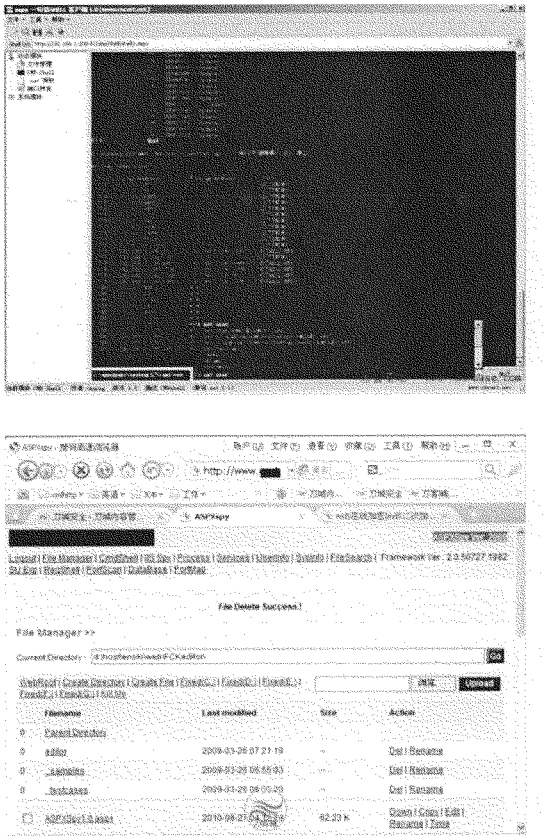


Figure 5. WebShell and ASPXSpy tools allow an attacker to bypass many firewall rules to funnel all control through a company's web server.

Once the initial system was compromised, the attackers compromised local administrator accounts and Active Directory administrator (and administrative users) accounts. The attackers often used common Windows utilities, such as SysInternals tools (acquired by Microsoft in 2006)—and other publicly available software, including hacking tools developed in China and widely available on Chinese underground hacker websites—to establish "backdoors" through reverse proxies and planted Trojans that allowed the attackers to bypass network and host security policies and settings. Desktop anti-virus and anti-spyware tools were also disabled in some instances—a common technique of targeted attacks.

Use of remote administration tools

Remote administration tools (RATs) are commonly used administrative tools that allow hackers (and administrators) to manage victims' computers (or managed systems) and completely control their use and function. A commonly used RAT in the hacker community is Gh0st and its many variants. RAT features often include screen and webcam spying, keystroke logging, mouse control, file/registry, and process management, and, of course, remote command shell capability.

McAfee has identified several RATs that have been used to establish a persistent infiltration channel into compromised companies. One of the most prevalent RATs is zwShell, which McAfee has seen in the wild since the spring of 2010 (compiled on 2010-03-17 08:47:00). Written in the Delphi language, zwShell was used by attackers to both build custom variants of the Trojan that they deployed on dozens of machines within each victim company, as well as to control compromised machines that would initiate beacon connections to it on a custom protocol.

Attackers used zwShell extensively to generate dozens of unique Trojan variants and to control the infected machines and exfiltrate sensitive data directly from them. (See Appendix A for a breakdown of the zwShell.)

Once the attackers had complete control of the targeted internal system, they dumped account hashes with gsecdump and used the Cain & Abel tool to crack the hashes to leverage them in targeting ever more sensitive infrastructures.

Files of interest focused on operational oil and gas field production systems and financial documents related to field exploration and bidding that were later copied from the compromised hosts or via extranet servers. In some cases, the files were copied to and downloaded from company web servers by the attackers. In certain cases, the attackers collected data from SCADA systems.

Detection

The methods and tools used in these attacks are relatively unsophisticated, as they simply appear to be standard host administration techniques, using standard administrative credentials. This is largely why they are able to evade detection by standard security software and network policies. Since the initial compromises, however, many individual unique signatures have been identified for the Trojan and associated tools by security vendors, including McAfee; yet only through recent analysis and the discovery of common artifacts and evidence correlation have we been able to determine that a dedicated effort has been ongoing for at least two years, and likely as many as four. We can now associate the various signatures to these events.

The following artifacts can help to determine whether a company has been compromised:

- Host files and/or registry keys
- Anti-virus alerts
- Network communications

Host Files and Registry Keys

Utility	Description
Command & control application	zwShell.exe 093640a69c8eafbc60343bf9cd1d3ad3 zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9
Trojan dropper	A packaged executable customized to each victim that includes the DLL file and configuration settings for installing the backdoor on the remote system. The dropper can be run from any directory and is usually executed with PSEXEC or an RDP session. Thus, related Windows Security Event logs provide useful information concerning compromised Active Directory accounts. These logs can be reviewed with Windows Event Log Manager or programs, such as "Event Log Explorer" or EnCase, which support search capabilities. When executed, the dropper creates a temporary file that is reflected in Windows update logs (KB*.log files in c:\Windows folder). This is because the Windows Registry is modified by the dropper to create a "netsvcs" key. Accordingly, the date of the backdoor installation can be determined from a search of the KB log files. This temporary file is also identified in the backdoor DLL itself. The temporary file is usually some alphanumeric combination that includes "gzg" (for example, xgt0gzg); however, it has been seen with generic file names (for example, server.exe) as well. The dropper is deleted when the backdoor is installed, and the temporary file is removed when the computer is restarted. If a backdoor has already been configured on the system, the dropper installation will fail unless it uses a different configuration.
Trojan backdoor	Dynamic link libraries (DLLs), also appearing under many other names. These files have a correlated Windows Registry key that is determined by the dropper when the backdoor is installed. The dropper iterates through the Windows netsvcs registry keys and uses the first available key, indicating the path and filename of the backdoor in a ServiceDLL register. The backdoor operates as a service through a "svchost.exe netsvcs –k" registry setting. The service key can be found under: HKLM\system\<controlset>\services\ The DLL is a system or hidden file, 19 KB to 23 KB in size and includes an XOR-encoded data section that is defined by the C&C application when the dropper is created. It includes the network service identifier, registry service key, service description, mutex name, C&C server address, port, and dropper temporary file name. The backdoor may operate from any configured TCP port. This DLL is specified in the ServiceDLL key in the related Windows netsvcs registry entry. The DLL is usually found in the %System%\System32 or %System%\SysWow64 directory.
Trojan backdoor 2*	startup.dll A6CBA73405C77FEDEAF4722AD7D35D60 Initially configured with the following: connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855 Connect.dll creates the temporary file "HostID.DAT," which is sent to the C&C server, then downloads and configures related DLLs including: • PluginFile.dll • PluginScreen.dll • PluginCmd.dll • PluginKeyboard.dll • PluginProcess.dll • PluginService.dll • PluginRegedit.dll Thereafter "Startup.dll" operates the service under a Windows Registry key. All communications seen so far with this version have been on ports 25 and 80 over TCP but can operate on any determined port. The service key is identified in the DLL (which does not include any encrypted data) as: HKLM\Software\RAT This DLL is usually found in the %System%\System32 directory; however, it has also been found in other locations. The path to the backdoor DLL is indicated in the Windows Registry ServiceDLL key.

*This DLL uses a different C&C application that may be an earlier version of zwShell, analysis continues.

The Trojan components are manually copied or delivered through administrative utilities to remote systems. They do not include any worm or self-replicating features, nor can the Trojan "infect" other computers. Removing the Trojan components is simply a matter of deleting the related files and registry settings.

The Trojan backdoor communicates with the C&C server at the address hard-coded in each DLL. The C&C server cannot modify the backdoor once it is installed; related systems must have the Trojan file removed before a new backdoor DLL can be installed on the system. Thus, if the C&C server address is changed, those servers that have the DLL with previous addresses must be remotely administered by the attacker.

Anti-virus Alerts

Anti-virus patterns are defined according to samples submitted by clients or analysts as they are discovered. Some Trojans exhibit characteristics of other types of malware, such as worms or viruses, that have the ability to infect other systems. RATs do not typically include such features, and, because they are defined with unique configurations for custom purposes, they commonly change faster than unique samples can be identified.

Only when an entire RAT toolkit is found can we define an anti-virus pattern that is generic enough to detect the RAT regardless of configuration changes. The package necessarily includes the C&C application server, the generator utility for creating droppers, related droppers, and backdoors—and a sufficient number of each to correlate the toolkit.

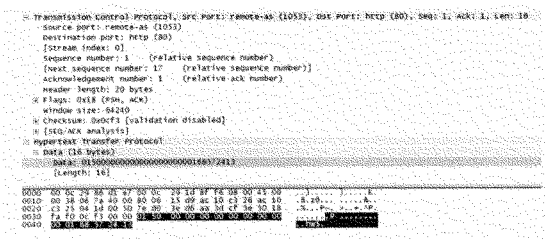
As mentioned previously, there have been several unique patterns developed from samples submitted to McAfee (as well as to other anti-virus vendors).

McAfee recommends that companies review McAfee ePolicy Orchestrator® (McAfee ePO™) software and anti-virus logs for "NightDragon" signature detections to identify related alerts since 2007 and then recover and resubmit these samples for analysis to investigate the related incidents. McAfee can assist with the analysis or provide instructions and tools for internal review.

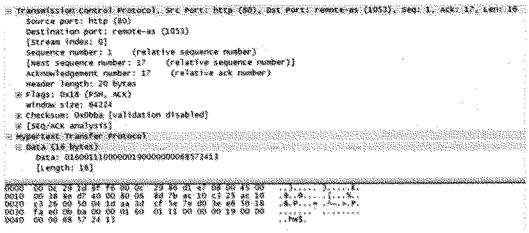
Network Communications

Network communications are relatively easy to detect because the malware uses a unique host beacon and server response protocol. Each communication packet between the compromised host and the C&C server is signed with a plain text signature of "hW$." (or "\x68\x57\x24\x13") at the byte offset 0x42 within the TCP packet.

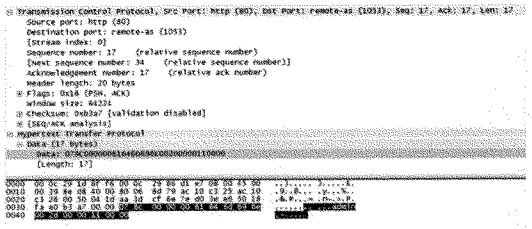
The backdoor begins its beacon at approximately five-second intervals with an initial packet that may be detected with the pattern: "\x01\x50[\x00-\xff]+\x68\x57\x24\x13."



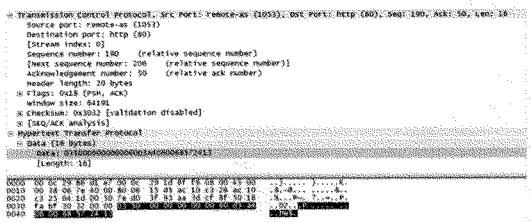
The server acknowledges the beacon with an initial response of "\x01\x60[\x00-\xff]+\x68\x57\x24\x13."



The backdoor sends the password to the server in clear text after the server acknowledges the connection.



While the backdoor and the server have an active connection, the backdoor will send "keep-alive" messages that can be detected with: "\x03\x50[\x00-\xff]+\x68\x57\x24\x13."



The attackers use "dynamic DNS" Internet name services accounts to relay C&C communications or temporarily associate DNS addresses with remote servers. Primary domains that have been used for C&C traffic include (all of these have been used frequently by other malware):

- [xxxx].is-a-chef.com
- [xxxx].thruhere.net
- [xxxx].office-on-the.net
- [xxxx].selfip.com

Note: The above hostnames (is-a-chef.com<http://is-a-chef.com>, thruhere.net<http://thruhere.net>, office-on-the.net<http://office-on-the.net>, selfip.com<http://selfip.com>) by themselves do not indicate malicious activity and there are plenty of legitimate subdomains that may use those hostnames. Communication to those hostnames should be carefully scrutinized but not necessarily raise alarm on its own

Company extranet servers have also been used as either unique or secondary/redundant C&C servers. In some instances, the attackers have (probably mistakenly) used droppers configured to compromise one company's computers—in another company's computers.

McAfee recommends that companies configure intrusion detection system (IDS) rules to detect the noted signatures (or employ the user-defined signature [UDS] "BACKDOOR: NightDragon Communication Detected" in McAfee Network Security Platform) and monitor DNS for outbound communications to dynamic DNS addresses resolving to or pathed back as suballocated to servers in China, where the company's name or common abbreviation forms the first part of the address. This may be difficult. However, if samples of the backdoor DLLs are found, DNS monitoring can help to identify other compromised hosts in the company network. McAfee also recommends that companies review web or IDS logs for file transfers to addresses registered in China. McAfee can assist with the analysis or provide instructions and tools for internal review.

Additional Detection Techniques

The backdoor beacons with its corresponding C&C server as long as the related address is active. If the address is abandoned or unreachable, the backdoor stops beaconing after some undetermined interval. When a compromised computer is restarted, however, the beaconing begins again because it is registered as a service in the Windows Registry. Anti-virus may or may not detect the Trojan unless it is beaconing or a full file system scan is performed.

McAfee Early Detection

Customers can deploy a number of McAfee products to help protect information systems from the Night Dragon attack:

- *McAfee Vulnerability Manager:* Using agentless discovery and vulnerability checking to assess systems on your network, McAfee Vulnerability Manager is an enterprise-class vulnerability management system that will detect infected Night Dragon systems as well as the security weaknesses in systems that have been compromised. The "wham-apt-nightdragon-detected-v7.fasl3" script will detect this threat remotely on systems.

- *McAfee Policy Auditor:* Using agent-based configuration audit checks to determine the most secure configuration of a system, McAfee Policy Auditor software detects the security weaknesses in the systems that have been compromised
- *McAfee Risk Advisory (MRA):* Properly deployed, McAfee Risk Advisor would have allowed administrators to see the misconfigurations and gap in security coverage that facilitated Night Dragon's exploitation

McAfee Detection

Night Dragon also displays a pattern of correlated activities with an assortment of other software tools that McAfee can assist companies to identify.

- *McAfee VirusScan Enterprise:* Update your anti-virus .DATs to at least version 6232 and ensure that on-demand scans are working properly and perform a full file system virus scan. Review McAfee ePO software or anti-virus alerts and network logs for "NightDragon" signature detections to identify compromised systems. Please submit any related samples to virus_research@mcafee.com or submit on the web at https://www.webimmune.net/default.asp.
- *McAfee Network Threat Response:* McAfee Network Threat Response technology would have detected the malicious C&C traffic and would have alerted administrators to the attack early, giving them time to react and prevent future damage

Administrators can also download the following free tools from McAfee:

- McAfee "Night Dragon Vulnerability Scanner" based on McAfee Vulnerability Manager technology to scan their networks for the presence of malware
- McAfee Labs Stinger

McAfee Prevention

For complete prevention of this and most other attacks involving advanced persistent threats (APTs), customers can deploy application whitelisting and change/configuration control software on their critical servers. These technologies completely prevent the unauthorized running of DLLs/EXEs as well as the modification of registry keys, services, and more involved in all of today's APT and zero-day attacks.

- *McAfee Application Control:* McAfee Application Control software stops Night Dragon by not allowing the dropper files from executing (even as administrator on Windows), thereby preventing downloads of additional malware and the setup of C&C channels that allowing RAT control and theft of sensitive files
- *McAfee Configuration Control:* McAfee Configuration Control software allows you to disallow any configuration changes to your systems, protecting them from being modified without explicit permission (even with administrative access)
- *McAfee Database Activity Monitoring:* delivers complete database protection including 0-day attacks and web born attacks such as those seen with SQL injection in Night Dragon.
- *McAfee Network Security Platform:* blocks malicious network activity such as APT command and control traffic.
- *McAfee Enterprise Firewall:* Properly installed and configured at the border and inside your organization, McAfee Firewall would have prevented the Night Dragon operation from penetrating so deeply into the affected organizations and would have blocked C&C communication from the RAT
- *McAfee Web Gateway:* Properly installed and configured, McAfee Web Gateway would have prevented the Night Dragon operation from using their RATs, requiring them to proxy-enable their RATs or use alternative proxy-enabled RATs
- *McAfee Endpoint Encryption:* Properly installed and configured, McAfee Endpoint Encryption software reduces the impact of the Night Dragon attack by restricting access to the core targeted assets

- *McAfee Data Loss Protection:* Properly installed and configured, McAfee Network DLP and/or McAfee Host DLP solutions allow you to prevent and detect the extraction of sensitive information from outside the company
- *McAfee Host Intrusion Prevention 8.0:* McAfee Host Intrusion Prevention 8.0 software has introduced a new "TrustedSource" APT detection feature that allows enterprises to correlate endpoint executable activity with the network C&C communication to detect and prevent RAT communications and data exfiltration activity
- *McAfee VirusScan® Enterprise:* In addition to detecting associated malware and RATs on the endpoint, customers can also leverage access protection features in McAfee VirusScan Enterprise to prevent (and alert on) the creation of Night Dragon-related files and folder structures. Other built-in features such infection tracing and McAfee Global Threat Intelligence™ can assist with the identification and quarantining or removal of new and unknown associated malware and RATs.

If you have discovered the presence of Night Dragon in your environment and would like incident-response or forensics assistance to respond and repair, please contact Foundstone Professional Services on incidentresponse@foundstone.com or submit any related samples to Virus_Research@avertlabs.com or on the web at McAfee Labs WebImmune.

Conclusion

Well-coordinated, targeted attacks such as Night Dragon, orchestrated by a growing group of malicious attackers committed to their targets, are rapidly on the rise. These targets have now moved beyond the defense industrial base, government, and military computers to include global corporate and commercial targets. While Night Dragon attacks focused specifically on the energy sector, the tools and techniques of this kind can be highly successful when targeting any industry. Our experience has shown that many other industries are currently vulnerable and are under continuous and persistent cyberespionage attacks of this type. More and more, these attacks focus not on using and abusing machines within the organizations being compromised, but rather on the theft of specific data and intellectual property. It is vital that organizations work proactively toward protecting the heart of their value: intellectual property. Enterprises need to take action to discover these assets in their environments, assess their configurations for vulnerabilities, and protect them from misuse and attack.

For additional research and information, review *Hacking Exposed: Network Secret and Solutions—6th Edition* (Osborne McGraw-Hill). You can also visit http://www.hackingexposed.com for information on advanced hacker techniques and to sign up for "Hacking Exposed" monthly webinars.

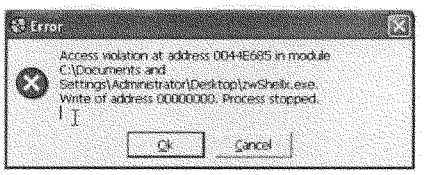
Credits and Acknowledgements

The preceding white paper was a collaborative effort among numerous people and entities including McAfee Foundstone Professional Services consultants, McAfee Labs, McAfee employees, executives, and researchers, HBGary and National Cyber-Forensics & Training Alliance (NCFTA). Significant contributors include Shane Shook, Dmitri Alperovitch, Stuart McClure, Georg Wicherski, Greg Hoglund, Shawn Bracken, Ryan Permeh, Vitaly Zaytsev, Mark Gilbert, Mike Spohn, George Kurtz, and Adam Meyers.

Appendix A: zwShell—the RAT

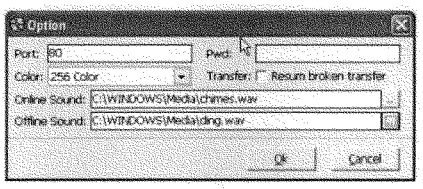
Below is a walk-through of the capabilities of zwShell and a demonstration of how the attackers used zwShell as a command and control server to exfiltrate data from within the targeted companies.

1. When zwShell is launched, it presents a fake crash error to the user and contains a hidden text entry field below the "Write of address 00000000. Process stopped" line. By entering the password in the hidden dialog box above the "ok" button to launch the application requires typing a special password, "zw.china." Without that password, the tool will not start. This obfuscation method is likely used to confuse investigators about the true purpose of this executable.

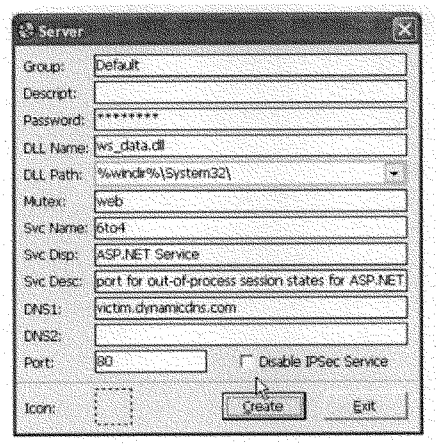


2. Once the error is bypassed, and zwShell is launched, it allows the attacker to create a custom Trojan by selecting the Server menu or to launch the C&C server by clicking Start and entering the port to listen for traffic with the password used by the backdoor DLLs. Once started, the application will begin listening for incoming compromised client connections and display them inside the grid. The attacker can launch as many instances of the zwShell application as required—as long as each listens to a different port or password. In this manner, multiple "networks" of compromised computers can be monitored.

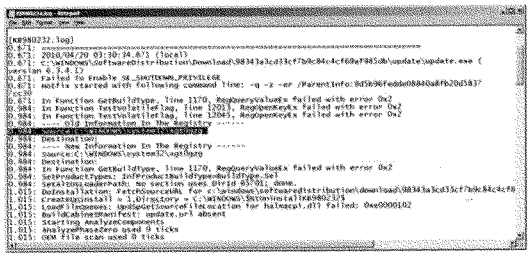
3. The attacker can also click on the Options menu to configure the C&C server settings. Those settings include selection of the listening port, the password that will encrypt the C&C traffic (which must match the password selected at the time of the Trojan generation), the ability to specify custom sound notifications for when infected machines connect and disconnect from the C&C server, and the ability to increase the color depth used for remote access to the machine, as well as an optional capability to allow resumes of interrupted file transfers from the client machine. The attacker can stop the listener and start with new options to monitor or connect with other compromised computers.



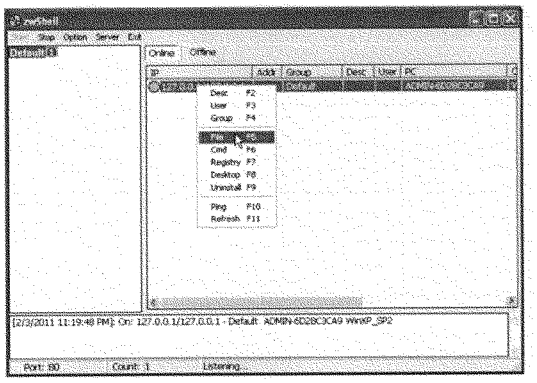
4. The attacker can specify the password (which must match the password set up for the server in Step 3), the name and path to the RAT DLL that will be injected into the svchost.exe Windows services process, the service and mutex names, and service displayed name and description. The attacker can also specify up to two C&C hostnames or IP address, port address, and dropper EXE process icon. Once the Create button is clicked, zwShell will generate a custom EXE dropper process which, when executed, will delete itself and extract a RAT DLL that will be launched as a persistent Windows service. The RAT will then immediately send a beacon on the configured port to the designated C&C server and wait for instructions.



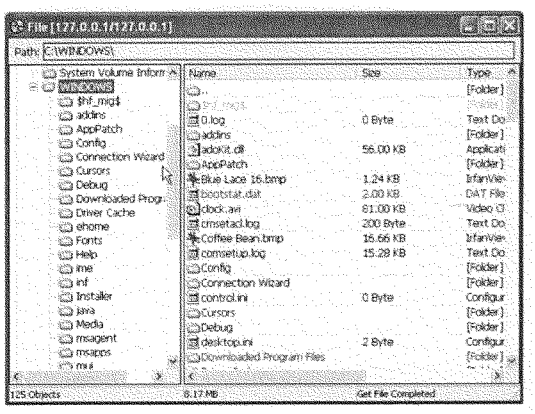
5. The dropper will be copied over network shares to the compromised computer and remotely execute with psexec or via Windows Terminal Services (RDP). In some cases, an "AT.job" or "SchTasks" entry will be used to execute the dropper over the network on the compromised computer. When executed, the dropper will create a temporary file and extract a RAT DLL that will be launched as a persistent Windows service. The RAT will then immediately send a beacon on the configured port to the designated C&C server and wait for instructions. The dropper will automatically delete itself after the backdoor service is created, and the temporary file will be deleted when the system is rebooted. An entry will be created in the Windows Update logs (KB****.log) in the C:\Windows directory with the date and time and path+name of the temporary file.



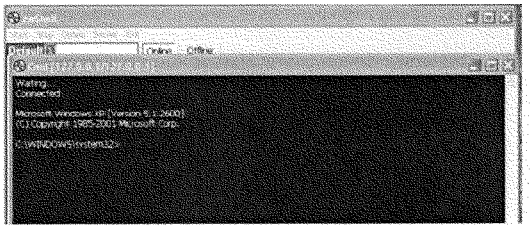
6. When a client is executed, it connects to the attacker's zwShell interface, along with its IP address, PC name, name of the logged-in user, and information about the operating system (OS) version of the machine, including the major patch levels.
7. The attacker in charge of the C&C server can establish full remote control of the connected machine and can browse the file system, launch command-line shells, manipulate the registry, view the remote desktop, and uninstall the Trojan from the client.



8. Browsing the client file system is a fully interactive process and has a familiar user interface similar to Windows Explorer. Individual files and folders can be deleted, renamed, copied, downloaded, and uploaded to the remote machine.



9. A remote command-line shell can be launched to execute commands directly on the remote machine. When the attacker uses this function, a copy of CMD.EXE is copied to the compromised system in a Windows %Temp% directory with the filename svchost.exe. This copy is an unmodified version of the Microsoft Windows command shell executable.



10. The Registry can also be viewed and edited in a user interface similar to the Windows Registry editor.

Appendix B: Attribution

IMPORTANT: McAfee has no direct evidence to name the originators of these attacks but rather has provided circumstantial evidence.

While we believe many actors have participated in these attacks, we have been able to identify one individual who has provided the crucial C&C infrastructure to the attackers—this individual is based in Heze City, Shandong Province, China. Although we don't believe this individual is the mastermind behind these attacks, it is likely this person is aware or has information that can help identify at least some of the individuals, groups, or organizations responsible for these intrusions.

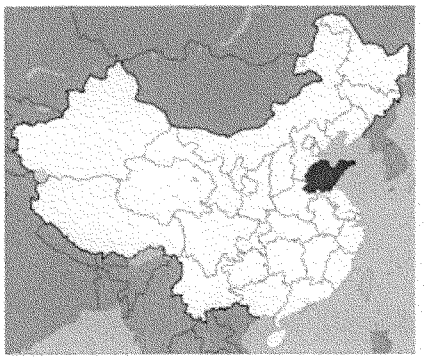


Figure 6. Shandong Province, China

The individual runs a company that, according to the company's advertisements, provides "Hosted Servers in the U.S. with no records kept" for as little as 68 RMB (US$10) per year for 100 MB of space. The company's U.S.-based leased servers have been used to host the zwShell C&C application that controlled machines across the victim companies.

Beyond the connection to the hosting services reseller operation, there is other evidence indicating that the attackers were of Chinese origin. Beyond the curious use of the "zw.china" password that unlocks the operation of the zwShell C&C Trojan, McAfee has determined that all of the identified data exfiltration activity occurred from Beijing-based IP addresses and operated inside the victim companies weekdays from 9:00 a.m. to 5:00 p.m. Beijing time, which also suggests that the involved individuals were "company men" working on a regular job, rather than freelance or unprofessional hackers. In addition, the attackers employed hacking tools of Chinese origin and that are prevalent on Chinese underground hacking forums. These included Hookmsgina and WinlogonHack, tools that intercept Windows logon requests and hijack usernames and passwords.

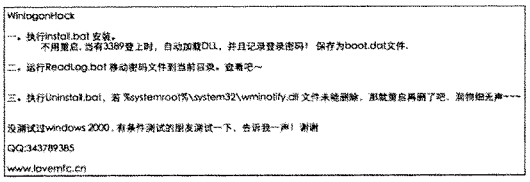


Figure 7. Instructions on the use of WinlogonHack tool by its Chinese developers.

On the compromised web server, they also deployed ASPXSpy, a web-based remote administration tool, also of Chinese origin.

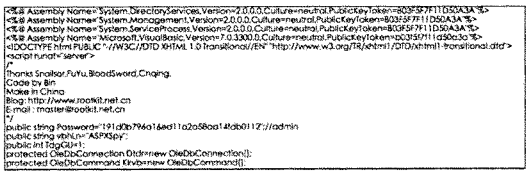


Figure 8. Parts of the ASPXSpy code with attribution to the Chinese developer.

There is nothing to suggest that the developers of these tools had any direct connection to these intrusions, as the tools are widely available on the Chinese web forums and tend to be used extensively by Chinese hacker groups. Although it is possible that all of these indicators are an elaborate red-herring operation designed to pin the blame for the attacks on Chinese hackers, we believe this to be highly unlikely. Further, it is unclear who would have the motivation to go to these extraordinary lengths to place the blame for these attacks on someone else. We have strong evidence suggesting that the attackers were based in China.

McAfee

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

21401wp_night-dragon_0211

Statement of Mr. Pablo A. Martinez
Deputy Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service

Before the Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism
U.S. Senate

April 12, 2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the role of the U.S. Secret Service (Secret Service) in investigating and dismantling criminal organizations involved in cyber crime.

On February 1, 2010, the Department of Homeland Security (DHS) delivered the Quadrennial Homeland Security Review (QHSR), which established a unified, strategic framework for homeland security missions and goals. The QHSR underscores the need for a safe and secure cyberspace:

> "Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services and resources. We know this interconnected world as cyberspace, and without it, we cannot communicate, travel, power our homes, run the economy, or obtain government services.
>
> Yet as we migrate more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. We face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services. For this reason, safeguarding and securing cyberspace has become one of the Department of Homeland Security's most important missions." (p. 29)[1]

[1] Department of Homeland Security. (2010). *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.*

In order to maintain a safe and secure cyberspace, we have to disrupt the criminal organizations and other malicious actors engaged in high consequence or wide-scale cyber crime.

As the original guardian of the nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

Due to our extensive experience investigating financial crimes, the Secret Service participated in the President's Comprehensive National Cyber Security Initiative to raise our overall capabilities in combating cyber crime and all forms of illegal computer activity. The Secret Service developed a multifaceted approach to combating cyber crime by: expanding our Electronic Crimes Special Agent Program; expanding our network of Electronic Crimes Task Forces; creating a Cyber Intelligence Section; expanding our presence overseas; forming partnerships with academic institutions focusing on cybersecurity; and working with DHS to establish the National Computer Forensic Institute to train our state and local law enforcement partners in the area of cyber crime. These initiatives led to the opening of 957 criminal cases and the arrest of 1,217 suspects in fiscal year 2010 for cyber crime related violations with a fraud loss of $507.7 million. The arrest of these individuals prevented an additional loss estimated at $7 billion dollars and involved the examination of 867 terabytes of data, which is roughly the equivalent of 867,000 copies of the Encyclopedia Britannica. As a result of these efforts, the Secret Service is recognized worldwide for our investigative and innovative approaches to detecting, investigating and preventing cyber crimes.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software and account takeovers leading to significant data breaches affecting every sector of the world economy.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting membership of approximately 80,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell and trade malicious software, spamming services, credit, debit and ATM card data, personal identification data, bank account information,

brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

Over the years, the Secret Service has infiltrated many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraudulent proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

In both of these cases, the effects of the criminal acts extended well beyond the companies compromised, affecting millions of individual card holders in one of the incidents. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Further, business costs associated with the need for enhanced security measures, reputational damage and direct financial losses are ultimately passed on to consumers.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems. An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The Secret Service investigation – the largest and most complex data breach investigation ever prosecuted in the United States – revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server

operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working with our law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[2] The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, resulting in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, TJX and Heartland investigations, as well as the recent apprehension of Vladislav Horohorin, were possible as a result of this valued partnership. The Secret Service looks forward to continuing our excellent work together.

The Secret Service also maintains an excellent relationship with the Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force where the FBI leads federal law enforcement efforts surrounding cyber matters of national security. In the last several years, the Secret Service has partnered with the FBI on various high-profile cyber investigations.

For example, in August 2010, a joint operation involving the Secret Service, FBI and the Security Service of Ukraine (SBU), yielded the seizure of 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of 85 terabytes of data, which was eventually transferred to law enforcement authorities in the United States. The data was seized from a criminal Internet service provider located in Odessa, Ukraine, also referred to as a "Bullet Proof Hoster." Thus far, the forensic analysis of these systems has already identified a significant amount of criminal information on numerous investigations currently underway by both agencies, including malware, criminal chat communications, and personally identifiable information of U.S. citizens.

[2] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

The case of Vladislav Horohorin is another example of successful cooperation between the Secret Service and its law enforcement partners around the world. Mr. Horohorin, one of the world's most notorious traffickers of stolen financial information, was arrested in Nice, France on August 25, 2010, pursuant to a U.S. arrest warrant issued by the Secret Service. Mr. Horohorin created the first fully-automated online store which was responsible for selling stolen credit card data. Working with our international law enforcement partners, the Secret Service identified and apprehended Mr. Horohorin as he was boarding a flight from France back to Russia. Both the CCIPS and the Office of International Affairs of the Department of Justice played critical roles in this apprehension. Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. We are presently awaiting Mr. Horohorin's extradition to the United States to face charges levied upon him in different districts by both the Secret Service and the FBI. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

One of the main obstacles that agents investigating transnational crimes encounter is the jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our international law enforcement counterparts. Currently, the Secret Service operates 23 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

The Secret Service also commends the efforts of both the Department of Justice and the FBI in working to address the "Going Dark" problem – the widening gap between the legal authority to intercept electronic communications pursuant to court order and providers' practical ability to actually intercept those communications. The Secret Service supports the written statements made by FBI Chief Counsel Valerie Caproni before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on February 17, 2011. As stated in her recent testimony, there are significant law enforcement challenges in light of the pace of technological advancements. Cyber criminals are at the forefront of exploiting these latest technological gaps to commit crimes.

Within DHS, the Secret Service has strengthened our relationship with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with US-CERT. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

The Secret Service is committed to ensuring that all its information sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Secret Service Framework

To protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- providing computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program**, and to our state and local law enforcement partners through the **National Computer Forensics Institute**;
- collaborating with our partners in law enforcement, the private sector and academia through our 31 **Electronic Crimes Task Forces**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Cyber Intelligence Section**;
- maximizing partnerships with international law enforcement counterparts through our **international field offices**; and
- maximizing technical support, research and development, and public outreach through the **Software Engineering Institute/CERT Liaison Program** at Carnegie Mellon University.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have

received extensive training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces

In 1995, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress further directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD of DHS, the State of Alabama and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Computer Emergency Response Team/Software Engineering Institute (CERT-SEI)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program to provide technical support, opportunities for research and development and public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; to provide an opportunity to work closely with CERT-SEI and Carnegie Mellon University; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI to publish the first ever "Insider Threat Study" examining the illicit cyber activity in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS S&T, are working to update the study. An updated study, expected to be released in late 2011, will analyze actual incidents of insider crimes from inception to prosecution. The research team will share its findings with federal, state, and local law enforcement, private industry, academia and other government agencies.

Conclusion

As more information is stored in cyber space, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted.

The Secret Service is committed to safeguarding the nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Subcommittee recognizes the magnitude of these issues and the evolving nature of these crimes.

Chairman Whitehouse, Ranking Member Kyl, and distinguished members of the Subcommittee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

STATEMENT OF JOHN E. SAVAGE

PROFESSOR OF COMPUTER SCIENCE

BROWN UNIVERSITY

BEFORE THE

COMMITTEE OF THE JUDICIARY

SUBCOMMITTEE ON

CRIME AND TERRORISM

UNITED STATES SENATE

HEARING ON CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM

"THE TECHNOLOGY/POLICY INTERSECTION"

APRIL 12, 2011

Chairman Whitehouse, Ranking Member Kyl, and honorable Members of the Subcommittee, my name is John Savage. I am a professor of computer science at Brown University where I teach and do research in computer science. Thank you for inviting me to speak to you on cybercrime and terrorism, two very important issues.

As a nation we have chosen to computerize a very large portion of our data and infrastructure. Consequently, important and valuable personal, business and government information is now available electronically. We have also become very dependent on computer networks in our daily lives and to run governments and businesses. Unfortunately, as we know, computers and networks are not secure, putting both data and networks at risk as well as our national economy. For example, in 2009 U.S. citizens lost $560 million to computer fraud.[1]

Criminals, commercial entities, terrorist groups and nation states may compromise deployed systems and steal confidential data, such as personal identities, intellectual property, and state secrets. The global reach of the Internet, while profoundly useful also simplifies their task, thus compounding the problem. In addition, important parts of our critical infrastructure have been integrated into the Internet without sufficient concern for the myriad security hazards that are introduced. Consequently, if a major conflict is played out in cyberspace, one of the first casualties will be our economy, a daunting prospect. However, the ramifications can go well beyond just economic considerations.

How bad is the problem?

Sophisticated users today can easily penetrate our computers. In their annual 2010 report[2] PandaLabs (a private computer security company) says that 46.8% of computers worldwide were compromised. That's almost half of all computers. In early 2010 PandaLabs, Defence Intelligence (another IT security company), the FBI and the Spanish Civil Guard announced that they shut down the Mariposa botnet, a global network of 12.7 million compromised computers, an absolutely huge number of machines under the control of one group. Botnets are potentially large collections of computer based agents, all working collectively to generate spam, conduct

[1] U.S Department of Justice, Internet Crime Report.
[2] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf

phishing expeditions, and run denial of service attacks, among other things. Phishing involves sending users messages that entice them into clicking on links, which downloads code and compromises their computers. A denial of service attack sends a flood of packets to one or a few web sites, overwhelming them and making them unavailable. This was done during the assault on Estonia in 2007 and as a precursor to the Russian invasion of Georgia in 2008.

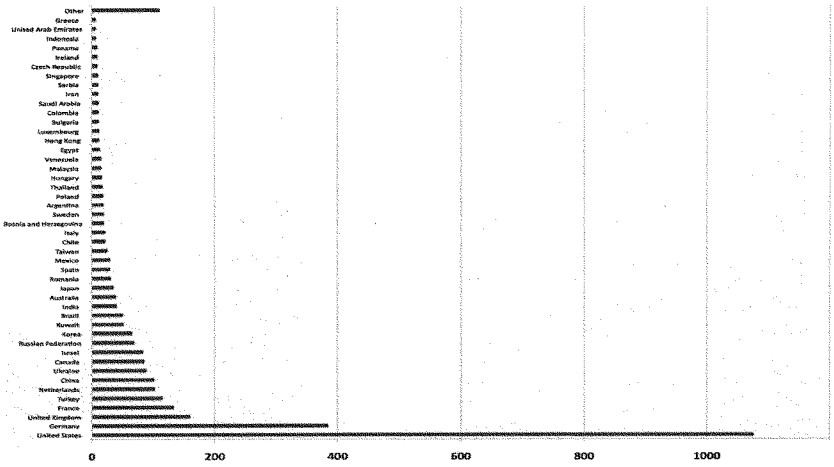
The computer industry knows that certain types of software error lead to theft, violations of privacy, and capture of the control of computers. For example, the MITRE Corporation with the assistance of the SANS Institute publishes a list[3] of the top 25 most dangerous software errors. And GFI Software reports[4] that seven of the top ten malware threats last November were Trojan horses, threats that grant complete control of a computer to an attacker.

Our networks and their support systems, such as the Domain Name System (DNS), are also vulnerable. They were designed on the assumption that individual users and network managers could be trusted to provide correct information when translating domain names, such as www.senate.gov, into IP addresses, strings of bits, and when circulating information about the available network paths. While it was reasonable to trust such information when the Internet was in its infancy, it isn't today. As a consequence, DNS attacks can not only send innocent users to malicious sites where their identities can be stolen, they can also result in traffic being routed to the wrong destinations.

An example of the latter type of attack was described in a recent paper[5] and press report[6] in which the authors claim that a 250,000-computer botnet could disrupt Internet routing globally. Imagine how much easier it would be to do this if a botnet of the size of the Mariposa botnet with almost 13 million computers were available. As shown in the graph below that was generated by Team Cymru[7] (an Internet security research firm), in January 2010 the U.S. had about three times as many botnets as any other nation.

---

[3] MITRE Corporation at http://cwe.mitre.org/top25/
[4] http://www.net-security.org/malware_news.php?id=1561
[5] **Losing Control of the Internet: Using the Data Plane to Attack the Control Plane**, Suchard et al, NDSS, 2011.
[6] **Death of the Internet, film at your local Cineplex**, I. van Beijnum, Ars Technica, March 21, 2011
[7] http://www.team-cymru.org/



What's to be done?

Computer industry insiders have solutions to many cyber security problems, but the incentives to adopt them are weak, primarily because security is expensive and there is no requirement they be adopted until disaster strikes. Nonetheless, many software companies, notably those who participate in BSIMM[8] (the Independent Software Vendors and the Financial Services Companies) have made great strides in eliminating software and system vulnerabilities that expose their products to attack. OWASP[9] plays a similar role for web-based security. Web applications offer some of the most challenging threats to identity management and theft. The fact that the cyber security problem remains a serious threat shows the need for much more research and development on the science and engineering of cyber security.

While waiting for research to bear more fruit, it makes sense for the U.S. government, together with the private sector, international partners, and independent agents, such as academics, to arrive at some reasonable software standards that all sufficiently large vendors selling software

[8] http://bsimm.com/online/
[9] https://www.owasp.org/index.php/Main_Page

in the U.S. should be required to meet. The same kind of standards could be developed and applied to the hardware vendors.

Although it is far preferable to protect systems in advance rather than patch them after vulnerabilities have been discovered, there is no alternative to requiring users to keep their software current. Because large botnets are a threat to national security, it is important to have some procedures in place to require inspection of computers to reduce the risk that they are compromised.

Protecting networks from hijackings (redirecting large volumes of traffic), man-in-the-middle attacks (intercepting traffic while en route to its destination), and routing disruptions require an entirely different set of steps. Problems of this kind are international in nature and must be handled that way. As noted in a 2009 National Academy of Sciences (NAS) study[10], it is unlikely that we can adequately secure the U.S portion of cyberspace without international engagement. Robert Knake, in a 2010 Council on Foreign Relations study[11], says that "The United States is being outmaneuvered in the international forums that will determine the future of the Internet" and warns that "nondemocratic regimes are ... promoting a vision of the Internet that is tightly controlled by states." Furthermore, he says protecting our interest in "an Internet as a platform for increased efficiency and economic exchange ... requires far more extensive engagement within Internet governance forums to shape the future of the network in a way that addresses security concerns without resulting in a cure that is worse than the disease."

In my opinion as a nation we should take seriously the recommendations of thoughtful observers on how best to engage the world community on this important topic while serving

[10] Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Academies, Press, 2009.
[11] Internet Governance in an Age of Cyber Insecurity, Robert Knake, Report No. 56, Council on Foreign Relations, September, 2010.

our national interests. Healthy discussions on methods to develop norms of behavior and rules of the road for safe and secure operation in cyberspace should be welcomed[12].

The research and development agenda

Coming back to the research dimension, as mentioned above, the good news is that progress has been made in making software more secure by design. However, not all software vendors are applying these safeguards to their products. Furthermore, there is a lot of old software in use that has not been designed with security in mind. Finally, new software vulnerabilities are being invented all the time. Research and development to protect systems are needed to cope with these realities.

Progress has also been made in addressing serious network problems. Recently three authors published a paper[13] showing that they can defend against a multimillion-node botnet denial of service attack. For example, if the Mariposa botnet were to be used to attack government or military networks, the attack could be thwarted with their technique. This is very good news. A major threat to operations, especially in our net-centric military would be mitigated. Solutions have also been found to the network flooding attack[14] mentioned above that is designed to disrupt Internet routing globally.

The *crypto computing problem*[15], posed in 1978, is whether or not it is possible to encrypt data in such a way that computations can done without ever decrypting the data. If the problem has a solution, and if an attacker penetrates a computer equipped to behave in this way, the information obtained would be useless unless the attacker also has the keys to decrypt it. This problem remained unsolved until May 2009 when Craig Gentry provided a first proof of concept[16]. The proof is too costly to implement commercially today, but it does provide hope that an efficient solution could be found eventually to the data theft problem. This is the common path that many breakthrough discoveries take. First we must know that a solution

[12] *Cyber Security and International Agreements*, Sofaer, Clark and Diffie, **Procs. Workshop on Deterring CyberAttacks**, National Academies, Press. 2010.
[13] **Phalanx: Withstanding Multimillion-Node Botnets**, Dixon et al, Proceedings NDSI'08, 2008.
[14] **Losing Control of the Internet: Using the Data Plane to Attack the Control Plane**, Suchard et al, NDSS, 2011.
[15] **On Data Banks and Privacy Homomorphisms**, Rivest et al, Foundations of Secure Computation, 1978.
[16] https://researcher.ibm.com/researcher/view_project.php?id=1548

exists then we find an efficient one. Recently[17] both the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Agency (IARPA), recognizing the potential of this work, have funded research designed to find more efficient solutions for this technique. However, this approach is vulnerable in the sense that a secure computer is needed to encrypt the program and data in the first place and then decrypt the results.

Conclusions

The problem of making our computers, networks and applications safe from attack is unsolved and probably will remain so for several reasons. First, human innovation is relentless, and especially if there is money to be made or an enemy to defeat. Second, security has been notoriously difficult to define. This is illustrated by the fact that a single-bit error can result in a system intrusion.

Given the above, can the cyber security problem be made manageable? My answer is "Yes." I liken our computers to our homes. A determined attacker can easily break into them. So why aren't most of our homes invaded more often? Apparently because the locks are good enough, the neighbors sufficiently vigilant, uniformed police officers sufficiently visible, and the punishment, if caught and convicted, sufficiently onerous to deter attackers. We need to arrive at a similar state in cyber. However, it cannot be done without more secure hardware and software, surveillance of the abuse of computers and networks, government regulation, international engagement and, possibly, the creation of an intergovernmental organization. Since it is better to build in security rather than try to add it after the fact (such as firewalls and intrusion detection), hardware and software vendors and network providers should be required to conform to reasonable cyber security guidelines.

Recommended Governmental Actions

- Explore proposals for effective international cooperation on the development of cyberspace norms and rules of the road.

[17] http://blogs.forbes.com/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/

- Develop a targeted cyber security research program to address at least the following topics:
    - Find methods of conducting intrusion surveillance that protect privacy
    - Support research to discover efficient solutions to the crypto computing problem
    - Fund research to make existing systems and networks more secure
- Support programs to produce policymakers knowledgeable about computer and networking technology and technologists who can cooperate with policymakers.

STATEMENT OF DR. PHYLLIS SCHNECK

VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

MCAFEE, INC.

BEFORE:

UNITED STATES SENATE

JUDICIARY COMMITTEE

SUBCOMMITTEE ON CRIME AND TERRORISM

"CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

APRIL 12, 2011

Chairman Whitehouse, Ranking Member Kyl and other distinguished members of the Subcommittee, thank you for requesting McAfee's views on responding to the threat of cyber crime and terrorism. Your subcommittee is playing a vital role in helping define the contours of the cyber security debate by investigating how we can defeat sophisticated syndicates of terrorists and criminals who deploy cyber attacks to finance their operations and undermine the security of our country.

My name is Phyllis Schneck and I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to serving as Vice President and Chief Technology Officer, Global Public Sector, for McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 300 cyber criminals worldwide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I have also served as a

commissioner and working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

Before discussing McAfee's views on security, I want to note that McAfee also takes privacy very seriously – both in terms of our customers' information and that of the systems and networks we secure. We are committed to abiding by privacy laws and directives in the multinational jurisdictions in which we do business. We also believe that by researching and implementing cutting edge technologies to secure information and systems, we are providing the foundation for privacy protection, which is good, strong security.

My testimony will focus on the following key areas:

- McAfee's commitment to partnering with the law enforcement community;
- The evolution of the cyber security threat landscape;
- McAfee's Technical Response to the Cyber Crime Challenge – Whitelisting and Global Threat Intelligence;
- Two major cyber security attacks, Operation Aurora and Night Dragon, and their implications for our nation's security; and
- Policy recommendations to support law enforcement and improve public/private sector information sharing that is essential to give the government the capabilities it needs to respond to the modern cyber security challenge.

First I would like to provide a little background on McAfee.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 100 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Evolution of the Cyber Security Threat Landscape

Traditionally, cyber crime has been associated with criminals using electronic means to obtain unauthorized access to financial information or money. Over time, the criminal landscape has evolved to include theft of intellectual property, network activism (e.g., distributed denial of service, or DDoS), and the destruction of critical infrastructure. Furthermore, the profit model continues to evolve and is getting even more lucrative for

cyber criminals, with a low barrier to entry and the prospect of significant monetary or strategic gains.

The evolving nature of cyber crime, and the context in which it operates, informs the way we define our company's strategy and design our products. My testimony, therefore, seeks to shed light on the way we think about cyber crime, how we drive the innovation of our products, and how we partner with the government to help make our country's networks and systems more resilient.

McAfee's Commitment to Partnering with the Law Enforcement Community

McAfee has a long history of collaborating with law enforcement at the global, federal, state and community levels, and our employees take great pride in this fact. Within the law, McAfee has assisted federal, state, and local police officials, supporting their investigations and prosecution of cyber criminals. We have worked to build strong working relationships with the FBI, U.S. Secret Service, state and local police, and governments worldwide that enable smooth, bi-directional communication both in times of crisis and during periods of normal operations. We help bridge these relationships for customers and partners by placing a particular focus on ensuring that coordination takes place when cyber events are occurring. In addition, we work to educate and get McAfee-developed information to law enforcement as quickly as possible.

As previously mentioned, I personally support law enforcement's efforts in cyber security, having served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program, and chairing for the past 10 years the Board of Directors for the National Cyber Forensics and Training Alliance. NCFTA is a non-profit organization that co-locates critical infrastructure fraud analysts with law enforcement to engage data analysis and collaboration between public and private sectors while also preserving chain of custody of any findings so they may be used by law enforcement in court. The work within NCFTA has led to over 300 arrests of cybercriminals worldwide.

McAfee also has played an active role in the Department of Homeland Security's (DHS) Cyber Storm 1, 2, and 3 exercises to enable the Department to model cyber attacks and improve their ability to respond to them. We collaborate closely with DHS and the National Cyber Security Alliance (NCSA) to educate consumers on cyber crime, and have developed a free citizen scanner to help citizens gauge their risk of online crime victimization. We maintain a free website that we have offered to the U.S. government to host as part of their cyber security awareness activities related to a national campaign, "Stop.Think.Connect." In addition, McAfee supports the National Strategy for Trusted Identities in Cyberspace (NSTIC), working with our partners in government and industry to enable innovation for more efficient authentication and other technologies that facilitate a safer and more pleasant experience for electronic transactions.

In addition to these activities, two years ago McAfee announced an initiative to fight cybercrime – a wide-ranging initiative aimed at closing critical gaps in assisting victims of cybercrime and preventing new events. This initiative is anchored by a multi-point plan that includes calls for action from law enforcement, academia, service providers, government, the security industry, and society at large to deliver more effective investigations and prosecutions of cybercrime.

Key elements of the initiative include:

- Education and Awareness – McAfee works to ensure that officials around the world have the understanding and capacity to properly fight cybercrime, while helping users build "street smarts" so that they don't become easy victims.
- Legal Frameworks and Law Enforcement – McAfee works to facilitate international collaboration and mutual assistance on cybercrime among governments, industry, and non-governmental organizations (NGOs).
- Innovation – McAfee works with the technology industry to provide technology solutions that stay one step ahead of the threats.

As part of our program, we maintain relationships with law enforcement communities around the world to facilitate information exchange, and we have trained numerous officers on malware creation and detection. What's more, we have provided grants to such key cybercrime fighters as the National White Collar Crime Center in the U.S. and the Council of Europe for its work on the Cybercrime Convention and outreach.

The Evolution of the Cyber Security Threat Landscape

For purposes of this testimony, we define malware as a set of instructions for a computer that causes the computer to behave according to the will of the malware owner, such as providing unauthorized access to information or systems that control physical/kinetic infrastructure. To put it simply, computers execute instructions. Malware puts the enemy's instruction next on the list, and then the adversary controls all actions forward, sometimes hiding its presence. Malware enters a machine from a variety of ports, typically email, web, or connection-level access that is unprotected or ill advised to admit these harmful instructions. Malware can also be referred to commonly as a "'virus." As in biology, when a machine has a virus, it is compromised, and its functions can cause harm.

Historically, security software relied on antivirus "signatures" to recognize and block malware. Upon detecting a virus, a security software vendor develops a signature and deploys it in the form of a file downloaded to the security software on customers' computers. That software is then in a position to recognize and block the malware – an approach much like a vaccine that requires advance knowledge of the threat. However, this approach is not sufficiently fast to fight today's cyber adversary, and that is why McAfee is changing the paradigm to proactive defense in real-time: to make our networks sufficiently intelligent to prevent malicious instructions from reaching the target – instead of requiring that the target be vaccinated with a signature.

Today, malware developers combine web, host, and network vulnerabilities with spam, rootkits, spyware, worms, and other means of attack. Significantly, malware is often distributed with micro-variations – known as polymorphism, or the ability to change

quickly – with the effect that a signature developed when the malware is first discovered is ineffective against the multiple, very slightly different forms of the same malware. This is analogous to a disease mutating so that the vaccine is no longer effective. Malware may be distributed indirectly by networks of computers that have been corrupted by a criminal – known as a "botnet."

Criminals and nation states can invest great efforts to deploy their software in hundreds of thousands, or indeed millions, of computers owned by innocent third parties, in order then remotely to command their botnet to launch an attack on a particular set of targets. The malicious software distributed by botnets will often actively evolve to become whatever is needed by its controller and is not limited by the boundaries of antivirus labels. This means that code that appears otherwise harmless in order to be let into the network can be told to spread rapidly – which is why we refer to this type of code as a worm. Thus malware originally configured to generate spam messages can be instructed to steal banking information. Again, cyber actions rely on the execution of instructions, and a compromised machine often follows the adversary's instructions to reach out to a server in another location for its next set of instructions, which can vary widely.

By leveraging multiple threat vectors, hackers are able to extend the time period in which their malware remains undetected and are able to steal the money, personal data, and other valuable information of users throughout the United States and the world. In this way, what might be called classic "viruses" have been blended in recent years with other types of malware and techniques used by malicious hackers intent on stealing personal data. Hackers have discovered that direct external attacks are unnecessary and risky. It is now easier to engineer malicious software that is delivered to a system remotely through various means and that can insidiously send information back indefinitely before being detected.

Modern malware, therefore, can no longer be classified by its perceived purpose or propagation method, because those change in an instant. Some types of software can be engineered to gain access to and maintain control over the victim's machine. Once the

malware is on the system, it seeks to communicate with its controlling entity – the criminal actor. And once communication is established over the Internet, any compromised machine can be instructed both to pass over any data of value to the criminal and to act as an instrument of attack against other computers and networks.

McAfee's Technical Response to the Cyber Crime Challenge: White Listing and Global Threat Intelligence

Because the traditional "signature" model for antivirus, analogous to requiring a vaccine for every piece of malware, is no longer effective to combat swiftly moving cyber adversaries, more advanced defenses are needed. To win back our network resiliency requires not only strong public-private collaboration, but also that we move at machine speed – at the speed of light – and that we stay ahead of the adversary. Thus the two most critical innovations for the future of cyber security are application whitelisting and global threat intelligence.

Whitelisting

Instead of relying only on preventing malware from entering a machine or requiring prior knowledge of a piece of malware (via anti-malware software or signature-based "blacklisting" products), whitelisting changes the entire paradigm. Whitelisting (also known as application whitelisting) simply does not permit the execution of any instruction set that has not been previously approved. Thus, even though the adversary may in fact be able to get malicious code onto a machine, that machine, if equipped with whitelisting technology, will never execute the malicious instructions. The analogy in biology is exposing a person to a disease that will never be able to develop or harm the person.

Whitelisting technology enables organizations to be much more proactive in protecting their systems. Trusted applications, system components, and executables are identified and explicitly allowed. All other software or executables are denied by default. The technology is used to protect servers, endpoints, embedded devices and mobile devices. Significantly, whitelisting can also protect the integrity of many ATM's, point-of-sale terminals, and Supervisory Control and Data Acquisition (SCADA) systems, which, because

of resource constraints, often might not support traditional anti-malware software.

Global Threat Intelligence (GTI)

The second critical technology in proactively fighting cyber crime is known as global threat intelligence. McAfee and other sophisticated cyber security providers have developed multi-vector, real-time, predictive protection against these more sophisticated attacks on information systems. McAfee's solution is called Global Threat Intelligence, or GTI. GTI is the basis of a cyber immune system: the ability to protect against an attack by electronically detecting – via correlation at machine speed – cyber behavioral data from worldwide sources that is identified as harmful, long before a signature or name might be developed at human speed. The biological analogy is the human body defending against a potential disease simply because the body detects that the behavior is harmful.

Cyber security solutions based on this GTI approach protect the customer's computer by calculating the potential risk of a piece of content based on experience with either the IP address from which it originates, the web site, or other elements associated with the content in question. Thus cyber security providers can offer solutions enabling the customer to stop content that has a risk probability score that, in the customer's view, is "too risky" to be loaded into the memory of the customer's computer.

McAfee's Global Threat Intelligence service, as well as a number of our other products and services, helped us first detect and then remediate two important recent global cyber security attacks – Night Dragon and Operation Aurora. These attacks are significant because they were managed by coordinated and organized teams that succeeded in extracting billions of dollars of intellectual property from leading global companies (many of which were American) in the information technology, defense, and energy sectors – strategic industries vital to the country's long-term economic success and national security.

Two major cyber security attacks: Operation Aurora and Night Dragon

Operation Aurora

On January 14, 2010 McAfee Labs identified a zero-day (previously publicly unknown) vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies. Microsoft has since issued a security bulletin and patch.

Operation Aurora was a coordinated attack that included a piece of computer code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit is then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, according to Google, additionally gain access to user accounts.

We also discovered that intruders used a social engineering message, known as "spear-phishing," to target employees with a high level of access in these companies (either software developers, quality assurance engineers, or domain administrators). The message would come from a previous acquaintance of the targeted user and would ask them to click on a web link pointing to a web server in Taiwan. As we uncovered and then reported to Microsoft, the web link hosted an obfuscated and encoded exploit for a zero-day vulnerability in Internet Explorer.

If a user had clicked on a link with Internet Explorer version 6, their machine would automatically be compromised and malicious code downloaded and executed stealthily on the computer. The Trojan would establish an evasive backdoor command and control channel to the same server in Taiwan through which live attackers would jump onto the system and proceed to escalate their privileges on the local machine as well as other servers within the network. As they moved rapidly through the network, the attackers would identify and compromise repositories of intellectual property and exfiltrate data of

interest out of the company. In many cases, this data included source code – the crown jewels of these information technology companies – which then could be used by attackers to discover new vulnerabilities in software used by the critical infrastructure industry, government agencies, and many other organizations across the globe. McAfee is continuing to work with multiple organizations that were impacted by Operation Aurora, as well as with various government agencies, to address this major supply chain attack in the US commercial sector.

Night Dragon

McAfee has identified a string of attacks designed to steal sensitive data from targeted organizations. Unlike opportunistic attacks, the perpetrators appear to be highly organized, premeditative, and motivated in their pursuits.

Night Dragon attacks are similar to Operation Aurora and other advanced persistent threats, or APTs, in that they employ a combination of social engineering and well-coordinated, targeted cyber attacks using remote control software and other malware. McAfee has linked these attacks to intrusions starting in November 2009, and there is circumstantial evidence suggesting they may have begun as early as 2007. Currently, new Night Dragon victims are being identified almost weekly.

Night Dragon attacks leverage coordinated, covert, and targeted cyber attacks involving social engineering; spear-phishing; vulnerability exploits in the Windows operating system; Active Directory compromises; and remote administration tools, or RATs. The attack sequence is as follows:

- Public-facing web servers are compromised via SQL injection (a code injection technique that exploits a security vulnerability in the database layer of an application); malware and RATs are installed.
- The compromised web servers are used to stage attacks on internal targets.

- Spear-phishing email attacks on mobile, VPN-connected workers are used to gain additional internal access.
- Attackers use password-stealing tools to access other systems – installing RATs and malware as they go.
- Systems belonging to executives are targeted for emails and files, which are captured and extracted by the attackers.

McAfee has evidence of Night Dragon malware infections in the Americas, Europe, and Asia. The Night Dragon attackers are currently targeting global oil, energy, and petrochemical companies with the apparent intent of stealing sensitive information such as operational details, exploration research, and financial data related to new oil and gas field bid negotiations. As we saw with the WikiLeaks document disclosures brought about by a malicious insider, sensitive data theft can be highly damaging beyond regulatory penalties and lost revenue. And unlike Stuxnet, the tools and techniques behind Night Dragon are not specific to critical infrastructure and can be used to launch attacks against any industry.

Policy Recommendations

As the previous examples demonstrate, combating cyber crime requires constant vigilance and sophistication on the technical side. The same is true for the law enforcement side – on which the burden falls for prosecuting such crimes. Yet law enforcement continues to lack the tools and resources needed to effectively train for and respond to cyber crime. And law enforcement's ability to seek and receive funding is often hampered by the difficulty of quantifying cyber crime. We therefore urge Congress, even in this period of budget austerity, to support the funding requests of our nation's law enforcement organizations, which are dedicated to fighting cyber crime.

In addition to more resources for law enforcement, we need more information sharing. Officials have made tremendous progress in the creation of information-sharing constructs comprising multiple agencies and the private sector. With good information, the

collaboration enabled by these constructs will help us achieve what the enemy already has: speed and alacrity of information sharing and acting on it for high impact.

In many cases, private sector companies can solve a cyber security puzzle by evaluating many disparate clues and are willing to share in the name of the greater good transcending competitive boundaries. Private companies need protected ways to share their big picture research findings more rapidly with the government without loss of trust or creation of material events for stockholders, so that the most significant cyber security information is expeditiously actionable. This is the human component of what Global Threat Intelligence does at machine speed. We need both in order to defeat cyber adversaries, whose aim is to harm our way of life.

Broad-based situational awareness is vital to securing our global cyber systems and ensuring our national security. Policies that enable companies and governments to work together, using global threat intelligence (e.g., combining cyber, energy, finance, and other data) to enhance correlation and predictive capabilities, are critical to real-time responsiveness within the network switching/routing fabric. The Lieberman-Collins-Carper bill, (S.413), supports such information sharing by requiring the government to share information – including threat analysis and warning information – with owners and operators regarding risks to their networks.

The U.S. Government has made tremendous progress in the past two years in building international relationships to enable better prosecution of cyber criminals. A policy framework that further supports the expansion of these relationships throughout our community of allies would help reduce the profit model for cyber criminals by making punishment more likely. Technical innovations such as whitelisting and global threat intelligence increase the barriers to entry and decrease the chance of success of a cyber-threat reaching or hitting the target. The correct blend of technology and policy will greatly diminish the reward model for cyber crime worldwide.

Conclusion

The cyber security challenge faced by our country is a serious matter that requires an evolution in both technology and the way both the public and private sectors collaborate. In order to mitigate the cyber adversary, intelligence must be collected and shared among machines – at the speed of light – and also among people. Each sector has its own set of core capabilities. Thus only the government can implement the complex set of organizational and policy responses necessary to counter the growing cyber security threat. Leading information technology companies and their customers are uniquely positioned to act as early warning systems that can identify and help address cyber security attacks as a real-time cyber immune system.

With the right industry-government collaboration, networks of the future can comprise intelligence and create resiliency by instantly rejecting harmful code in milliseconds as opposed to the hours it traditionally takes to make a signature, just as our bodies reject viruses even though we may not know the name of the particular disease. Information technology companies focused on cyber security in particular have the resources and the economic incentives to continue to invent and develop the technologies and solutions needed to stay ahead of sophisticated cyber attackers. In the best American tradition of collaboration, the public and private sectors have made important strides to address the cyber security challenge and to enhance trusted working relationships. As we work together to further evolve our collaboration models, we can succeed in protecting our homeland from the threat of cyber attacks.

Thank you for asking me to participate in this hearing on behalf of McAfee. I would be happy to answer your questions.

Department of Justice

STATEMENT OF

GORDON M. SNOW
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
CRIME AND TERRORISM SUBCOMMITTEE

ENTITLED

"CYBERSECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

PRESENTED

April 12, 2011

Good afternoon Chairman Whitehouse, Ranking Member Kyl, and members of the Subcommittee. I'm pleased to appear before you today to discuss the cyber threats facing our nation and how the FBI and our partners are working together to protect United States (U.S.) government and private sector networks.

Countering efforts by foreign countries to steal our nation's secrets, evaluating the capabilities of terrorists in a digital age, and fighting cyber crime are the FBI's highest priorities. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies.

The Cybersecurity Threat

As the Subcommittee is aware, the number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow.

The threat has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet.

It is difficult to state with confidence that our critical infrastructure—the backbone of our country's economic prosperity, national security, and public health—will remain unscathed and always be available when needed.

The recent security breach by unauthorized intruders into the parent company of NASDAQ is an example of the kind of breaches directed against important financial infrastructure and illustrates the difficulty of determining clear attribution. As we would in response to any such breach, the FBI is working to identify the scope of the intrusion and assist the victim in the remediation process.

The FBI has identified the most significant cyber threats to our nation as those with high intent and high capability to inflict damage or death in the U.S., to illicitly acquire assets, or to illegally obtain sensitive or classified U.S. military, intelligence, or economic information.

As both an intelligence and law enforcement agency, the FBI can address every facet of a cyber case—from collecting intelligence on the subjects in order to learn more about their networks, to dismantling those networks and prosecuting the individual perpetrators. The ability to take action on the information we collect is critical because what may begin as a criminal investigation may become a national security threat.

In addition, the FBI's presence in Legal Attachés in 61 cities around the world assists in the critical exchange of case related information and the situational awareness of current threats, helping to combat the global scale and scope of cyber breaches. The FBI is also changing to adapt to the ever-evolving technology and schemes used by cyber criminals. Intelligence now drives operations in the FBI. The Bureau is working in new ways with long-standing and new partners to address the cybersecurity threat.

Cyber Threats Against the Private Sector

Cyber criminal threats to the U.S. result in significant economic losses. But the threat against financial institutions is only part of the problem. Also of serious concern are threats to critical infrastructure, the theft of intellectual property, and supply chain issues.

Cyber Threats to U.S. Critical Infrastructure

U.S. critical infrastructure faces a growing cyber threat due to advancements in the availability and sophistication of malicious software tools, and the fact that new technologies raise new security issues that cannot always be addressed prior to adoption. The increasing automation of our critical infrastructures provides more cyber access points for adversaries to exploit.

New "smart grid" and "smart home" products, designed to provide remote communication and control of devices in our homes, businesses, and critical infrastructures, must be developed and implemented in ways that will also provide protection from unauthorized use. Otherwise, each new device could become a doorway into our systems for adversaries to use for their own purposes.

Industrial control systems (ICSs), which operate the physical processes of the nation's pipelines, railroads, and other critical infrastructures, are at elevated risk of cyber exploitation.

The FBI is concerned about the proliferation of malicious techniques that could degrade, disrupt, or destroy critical infrastructure. Although likely only advanced threat actors are currently capable of employing these techniques, as we have seen with other malicious software tools, these capabilities will eventually be within reach of all threat actors.

Intellectual Property Theft and Supply Chain Risks

Intellectual property rights (IPR) violations, including theft of trade secrets, digital piracy, and trafficking counterfeit goods, also represent high cyber criminal threats, resulting in losses of billions of dollars in profits annually. These threats also pose significant risk to U.S. public health and safety via counterfeit pharmaceuticals, electrical components, aircraft parts and automobile parts.

Cyber crime that manipulates the supply chain could pose a threat to national security interests and U.S. consumers. Poorly manufactured computer chips or chips that have been salvaged and repackaged infringe on intellectual property rights and could fail at critical times, posing a serious health and safety threat to U.S. citizens. Malware could be embedded on the chips to exfiltrate information from computers and result in the theft of Personally Identifiable Information (PII) that could then be used in future cyber crimes. As the quality of counterfeit goods increases, U.S. consumers may be challenged to tell the difference between authentic and fraudulent goods.

Operation Cisco Raider is a joint initiative between the U.S. and Canada that targets the illegal distribution of counterfeit network hardware manufactured by private entities in China. The use of counterfeit network components can lead to exploitation of cyber infrastructure vulnerabilities and even network failure. Since 2006, Operation Cisco Raider has seized over 3,500 network components amounting to $3.5 million of Cisco retail products. Ten individuals have been convicted as a result of the joint initiative.

The Booming Business of Botnets

Botnets are networks of compromised computers controlled remotely by an attacker. Criminals use botnets to facilitate online schemes that steal funds or data, to anonymize online activities, and to deny access by others to online resources. The botnets run by criminals could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure. Today's botnets are often modular and can add or change functionality using internal update mechanisms.

Today's cyber criminals are business savvy. These criminals are building businesses based on the development, management, and sale of botnets. These criminal groups have programmers who write the malicious software, salespeople who sell the code or lease out botnet services, and, in some instances, dedicated support personnel. These criminals are working to make botnets easier to deploy and more difficult to detect.

Successful botnet development and operations use techniques similar to legitimate businesses including the involvement of personnel with various specialties, feature-based pricing structures, modularization, and software copy protection. The development and sale of kit-based botnets has made it easier for criminals with limited technical expertise to build and maintain effective botnets. Botnet development and management is approached in a business-like fashion. Some criminals rent or sell their botnets or operate them as a specialized portion of an ad hoc criminal organization. At least one botnet kit author implemented a copy protection scheme, similar to major commercial software releases, which attempts to limit unauthorized use of the botnet kit.

Botnets that specialize in data exfiltration are able to capture the contents of encrypted webpages and modify them in real time. When properly configured, criminals can ask additional questions at login or modify the data displayed on the screen to conceal ongoing criminal activity. Criminals purchase the base kits for a few thousand dollars and can pay for additional features to better target specific webservices.

The "Not for Profit" Cyber Criminal

Hacktivist groups such as 'Anonymous' undertake protests and commit computer crimes as a collective unit. Anonymous does not have a leader or a controlling party but instead relies on the collective power of individual participants. Its members utilize the Internet to communicate, advertise, and coordinate their actions. Anonymous has initiated multiple criminal Distributed Denial of Service (DDoS) attacks against the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), the Church of Scientology, and various businesses in support of WikiLeaks.

Just last month, Anonymous hacked into the website of a U.S. security firm with U.S. government contracts and stole approximately 72,000 e-mails from the company and posted them online. This attack was in response to the claim that a researcher at the company had identified key members of Anonymous.

Financial Estimates of Damages

Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into compromising their own systems. Once a system is compromised, cyber criminals will use their accesses to obtain PII, which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber crime is not felt equally across the board. A small company may not be able to survive even one significant cyber attack. On the other hand, companies may not even realize that they have been victimized by cyber criminals until weeks, maybe even months later. Victim companies range in size and industry.

Often, businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised, so they absorb the loss, making it impossible to accurately calculate damages.

As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates. Over the past five years, estimates of the costs of cyber crime to the U.S. economy have ranged from millions to hundreds of billions. A 2010 study conducted by the Ponemon Institute estimated that the median annual cost of cyber crime to an individual victim organization ranges from 1 million to 52 million dollars.

According to a 2011 publication released by Javelin Strategy and Research, the annual cost of identity theft is $37 billion. This includes all forms of identity theft, not just cyber means. The Internet Crime Complaint Center (IC3), which aggregates self-reported complaints of cyber crime, reports that in 2010, identity theft schemes made up 9.8% of all cyber crime.

Addressing the Threat

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the administration, we are devoting significant resources to this threat. Our partnerships within industry, academia, and across all of government have also led to a dramatic improvement in our ability to combat this threat.

The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists.

The FBI is a substantial component of the Comprehensive National Cybersecurity Initiative (CNCI), the interagency strategy to protect our digital infrastructure as a national security priority. Through the CNCI, we and our partners collaborate to collect intelligence, gain visibility on our adversaries, and facilitate dissemination of critical information to decision makers.

The FBI has cyber squads in each of our 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners. We have increased the capabilities of our employees by selectively seeking candidates with technical skills and enhancing our cyber training.

In addition, as part of the FBI's overall transformation to an intelligence-driven organization, the Cyber Division has implemented Threat Focus Cells, which bring together subject matter experts from various agencies to collaborate and address specific identified cyber threats.

Partnerships

However, one agency cannot combat the threat alone. Through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), we coordinate our efforts with 20 law enforcement and Intelligence Community (IC) entities, including the Central Intelligence Agency (CIA), Department of Defense (DoD), DHS, and NSA. The FBI also has embedded cyber staff in other IC agencies through joint duty and detailee assignments.

We have also enhanced our partnership with DHS, forming joint FBI-DHS teams to conduct voluntary assessments for critical infrastructure owners and operators who are concerned about the network security of their ICSs. DHS has provided more than 30 FBI agents and intelligence analysts with specialized training in these systems.

In addition, because of the frequent foreign nexus to cyber threats, we work closely with our international law enforcement and intelligence partners.

We currently have FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations: Estonia, the Netherlands, Romania, Ukraine, and Colombia. These cyber personnel have identified cyber organized crime groups targeting U.S. interests and supported other FBI investigations. We have trained foreign law enforcement officers from more than 40 nations in cyber investigative techniques over the past two years.

We have engaged our international allies, including Australia, New Zealand, Canada, and the United Kingdom, in strategic discussions that have resulted in increased operational coordination on intrusion activity and cyber threat investigations.

Government and Private Sector Information Sharing

The FBI has developed strong relationships with private industry and the public. InfraGard is a premier example of the success of public-private partnerships. Under this initiative, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, we have seen this initiative grow from a single chapter in the Cleveland field office to more than 86 chapters in 56 field offices with 42,000 members.

The exchange of knowledge, experience, and resources is invaluable and contributes immeasurably to our homeland security. Notably, DHS has recognized the value of the program and recently partnered with the InfraGard program to provide joint training and conferences during this fiscal year.

With outside funding from DHS, the newly formed Joint Critical Infrastructure Partnership will host five regional conferences this year along with representation at a number of smaller venues. The focus of the program is to further expand the information flow to the private sector by not only reaching out to the current InfraGard membership but also reaching beyond current members to local critical infrastructure and key resource owners and operators. The goal is to raise awareness of risks to the nation's infrastructure and to better educate the public about infrastructure security initiatives. This partnership is a platform which will enhance the risk management capabilities of local communities by providing security information, education, training, and other solutions to protect, prevent, and respond to terrorist attacks, natural disasters, and other hazards, such as the crisis currently facing Japan. Ensuring that a country's infrastructure is protected and resilient is key to national security.

Experience has shown that establishing rapport with the members translates into a greater flow of information within applicable legal boundaries, and this rapport can only be developed when FBI personnel have the necessary time and resources to focus on the program. This conduit for information results in the improved protection of the infrastructure of the U.S.

In addition to InfraGard, the FBI participates in other activities with the private sector, like the Financial Services Information Sharing and Analysis Center (FS-ISAC). A good example of this cooperation is the FBI's identification of a bank fraud trend in which U.S. banks were unaware that they were being defrauded by businesses in another country. As a result of FBI intelligence analysis, a joint FBI/FS-ISAC document was drafted and sent to the FS-ISAC's membership, alerting them to these crimes and providing recommendations on how to protect themselves from falling victim to the same scheme.

In the last few years, there has been a push to partner FBI intelligence analysts with private sector experts. This is an opportunity for the intelligence analysts to learn more about the industries they are supporting. They then can better identify the needs of those industries as well as FBI information gaps. Additionally, they develop points-of-contact within those industries who can evaluate and assist in timely analysis, and the analysts mature into subject matter experts.

Other successful cyber partnerships include the Internet Crime Complaint Center (IC3) and the National Cyber-Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. Complaints are referred to local, state, federal and international law enforcement and are also the basis for intelligence products and public service announcements. The FBI's IC3 unit works with the private sector, individually and through working groups, professional organizations, and InfraGard, to cultivate relationships, inform industry of threats, identify intelligence, and develop investigative information to enhance or initiate investigations by law enforcement.

The NCFTA is a private nonprofit organization, composed of representatives of industry and academia, which partners with the FBI. The NCFTA, in cooperation with the FBI, develops responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. The NCFTA work products can be provided to industry, academia, law enforcement, and the public as appropriate.

The FBI also partners with the U.S. private sector on the Domestic Security Alliance Council (DSAC). This strategic collaboration enhances communications and promotes effective exchanges of information in order to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

The DSAC is in a unique position to speak on behalf of the private sector because the DSAC members are the highest ranking security executives of the member companies, who directly report to the leaders of their organizations.

Successes

Our partnerships and joint initiatives are paying off, especially in the national security realm. In 2010, the FBI strengthened our efforts to counter state-sponsored cyber threats, increasing the number of national security computer intrusion cases by 60%.

While we increased our emphasis on national security, we continued to see successes on the criminal side. In 2010, we arrested a record 202 individuals for criminal intrusions, up from 159 in 2009. We obtained a record level of financial judgments for such cases of $115 million, compared to $85 million in 2009. Those arrests included five of the world's top cyber criminals. Among them were the perpetrators of the Royal Bank of Scotland (RBS) WorldPay intrusion. Due to our strong partnership with the Estonian government on cyber matters, the case resulted in one of the first hackers extradited from Estonia to the United States.

Conclusion

As the Subcommittee knows, we face significant challenges in our efforts to combat cyber crime. In the current technological environment, there are numerous threats to private sector networks, and the current Internet environment can make it extremely difficult to determine attribution.

We are optimistic that by strengthening relationships with our domestic and international counterparts, the FBI will continue to succeed in identifying and neutralizing cyber criminals, thereby protecting U.S. businesses and critical infrastructure from grave harm.

To bolster our efforts, we will continue to share information with government agencies and private industry consistent with applicable laws and policies. We will continue to engage in strategy discussions with other government agencies and the private sector to ensure that American ingenuity will lead to new solutions and better security. We will continue to build a skilled workforce to operate in this challenging environment.

We look forward to working with the Subcommittee and Congress as a whole to determine a successful course forward for the nation that allows us to reap the positive economic and social benefits of the Internet while minimizing the risk posed by those who would use it for nefarious purposes.

Department of Justice

STATEMENT OF

JASON WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
CRIME AND TERRORISM SUBCOMMITTEE

ENTITLED

"CYBERSECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

PRESENTED

April 12, 2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and Members of the Subcommittee. It is a pleasure to appear before you to testify about ensuring our nation's cybersecurity. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall cybersecurity strategy and enforcement efforts. In light of the FBI's participation on the panel, I will limit my remarks primarily to the ways in which other components of the Justice Department address cybersecurity issues.

Our society's reliance on digital infrastructure requires that not only the information infrastructure itself, but also all of the data it carries and activity that it supports be protected. The Administration is committed to integrating and organizing the government's cybersecurity efforts to better ensure that we have a comprehensive framework in place that will allow us to bring all appropriate tools to bear against cyber criminals, terrorists, and other malicious actors. The Department of Justice plays a key role in that fight.

As the Administration's 60-Day Cyber Policy Review recognized, the Department, through its prosecutorial and law enforcement components, and in partnership with other agencies, plays a critical role in cybersecurity by identifying the offenders, seizing their hardware and assets, and deterring their conduct through arrest and appropriately severe punishment. Its role in threat reduction and attribution works in concert with the roles of other agencies and private sector entities that focus on hardening targets and reducing vulnerabilities. Stated another way, we need to develop better locks, but when those locks are broken—as they inevitably will be—the Department responds to bring the offenders to justice.

Nature of the threat

As you know, the United States depends upon the information and communications infrastructure to conduct commercial, financial, personal, and governmental transactions. We face ongoing threats to the security of that infrastructure from a wide range of actors, including nation-states, criminals, and terrorists who exploit our pervasive dependency on information technology to misappropriate or destroy information, steal money, and threaten basic services, including those provided by critical infrastructures.

Ten years ago, many of the threats to the burgeoning Internet came from solo hackers, writing viruses like "I love you" or "Melissa," or crafting denial of service attacks on fledgling Internet companies. As troubling as those attacks were, the threats today are much more significant. We face the challenges of organized crime, botnets, identity theft, and carding, to name just a few. Many of these threats are based or originate overseas.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled hackers are now able to perpetrate large-scale data breaches that leave hundreds of thousands—and in many cases, tens of millions—of

individuals at risk of identity theft. Today's criminals can remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including personal financial information.

Online threats may take many forms, including "carders" and "phishers." "Carding" encompasses not only the unauthorized use of credit and debit card account information to fraudulently purchase goods and services, but also a growing assortment of related activities including computer hacking, phishing, cashing out stolen debit card numbers, re-shipping schemes, and Internet auction fraud. Through carding activity, which has become a growing problem in recent years, large volumes of data are stolen, resold, and ultimately used by criminals to commit fraud.

"Phishing" refers to an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Carders and phishers, among other types of cyber criminals, comprise a criminal underground in the cyber world that is dedicated to stealing and exploiting identity and financial information. Many of the actors in this criminal underground are outside of our national borders.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A report just released by McAfee and Science Applications International Corporation confirms this trend in cybercrime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product planning documents. These threats come both from outside hackers as well as insiders who gain access to critical information from within companies and government agencies.

The massive proceeds from these online crimes create another troubling issue. It is too soon to say where that money ends up, but the risk that it could be used to influence foreign governments, distort foreign justice systems, and fund terrorists cannot be ignored.

Let me give you an example of the kind of criminals that we are up against: organized, international, and profit-driven. In October 2009, nearly 100 people were charged in the U.S. and Egypt as part of an operation known as Phish Phry—one of the largest cyber fraud phishing cases to date and the first joint cyber investigation between Egypt and the United States. Phish Phry was the latest action in what Director Mueller described as a "cyber arms race" where law enforcement must coordinate and collaborate in order to keep up with its cyber adversaries. The defendants in Operation Phish Phry targeted U.S. banks and victimized hundreds of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled. More than 50 individuals in California, Nevada, and North Carolina and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identity theft. Led by the

FBI, this investigation required close coordination with state and local law enforcement, the Secret Service, and our Egyptian counterparts. In late March, five more people were convicted of federal charges for their roles in this "phishing" operation, bringing the total number of convictions to date to 46.

Role of the Department of Justice

The Department works closely with our partners throughout the government—including law enforcement agencies, the Intelligence Community, the Department of State, the Department of Homeland Security (DHS), and the Department of Defense—to provide legal support to cybersecurity efforts, inform policy discussions and ensure coordination of international efforts. The intersection between laws and technology can require complicated analysis and multidisciplinary training. That is why the Department has criminal lawyers, as well as attorneys working on national security matters, who are specially trained to handle cyber issues, ranging from the use of existing legal tools and authorities, to the ways in which we can vigorously protect privacy and civil liberties while still achieving our goal of securing the Nation's cyberspace.

Our work does not stop at our shores. Due to the global nature of the Internet, many of our cases involve computers located in other countries. Many times the offenders are located in another country. But even U.S. criminals will use computers located in another country to hide their tracks. Often it is impossible to identify, arrest, and prosecute offenders without the assistance of foreign governments. Due to the transnational nature of most cybersecurity incidents, achieving effective multilateral cooperation in real time has become a priority, which in turn has meant a higher priority for Department participation in US government delegations to various international bodies.

To assist us in preserving and obtaining data from other nations, the Department has engaged in numerous efforts to help address cybercrime problems around the world, including:

- promoting the Budapest Convention (Council of Europe Convention on Cybercrime), to which the U.S. is a party, and
- using State Department Foreign Assistance funds to provide capacity-building training and technical assistance to developing countries, including advice on developing their legal frameworks in this area, and
- promoting the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid law enforcement coordination across borders.

In the interagency context, the Department is currently providing legal and policy support to the Department of Homeland Security in support of its cybersecurity mission and the National Security Agency in support of its information assurance efforts. We are participating in

government-wide planning and preparedness efforts, such as the development of the National Cyber Incident Response Plan and the associated Cyber Unified Coordination Group, which assists the Secretary of DHS in coordinating responsive measures to significant cyber incidents, and cyber exercises such as Cyber Storm III.

Finally, the Department plays a leading role in counter-intelligence and national security investigations that uncover threats to our computer networks. Through the Department's National Security Division (NSD), we investigate, prevent, and prosecute where appropriate, the cyber activities of nation-states and terrorists that pose a threat to our national security. In addition, NSD exercises oversight authority over foreign intelligence collection efforts within the United States.

Enforcement

One key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals—with the goal of incapacitating or deterring them before they can complete an attack on our networks, or punishing them and deterring similar future acts if there is a successful intrusion.

The Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cyber crime wherever it occurs. The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), together with a nationwide network of 230 Computer Hacking and Intellectual Property (CHIP) prosecutors in our United States Attorney's Offices (USAOs), take a leading role in promoting and leading our efforts to investigate and prosecute cyber offenses. These prosecutors, as well as other prosecutors working cybercrime cases throughout the country, work closely with our law enforcement partners, including the FBI, the Secret Service, and the U.S. Postal Inspection Service. In addition, we have a strong partnership with the National Cyber Investigative Joint Task Force, which brings together law enforcement, intelligence, and defense agencies to focus on high-priority cyber threats.

Other sections of the Criminal Division also play important roles in cybersecurity. The Fraud Section focuses on large-scale fraud cases involving identity theft. The Office of International Affairs (OIA) supports and enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives.

Litigating components of the Department's National Security Division—the Counterespionage and Counterterrorism Sections—share the Criminal Division's and the USAOs' responsibility for safeguarding the country's information systems through enforcement of criminal laws. The Counterespionage Section prosecutes misappropriation of intellectual property to benefit a foreign government, as provided by the Economic Espionage Act of 1996 (18 U.S.C. § 1831), and obtaining national defense, foreign relations, or restricted data by accessing a computer without authorization, as provided by the Computer Fraud and Abuse Act

(18 U.S.C. § 1030). The Counterterrorism Section—leveraging the capabilities and expertise of CCIPS, CHIP prosecutors, the Anti-Terrorism Advisory Council, and Joint Terrorism Task Forces—would play a pivotal role in addressing any major cybersecurity attack by terrorists or associated groups or individuals.

Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, and the robust cooperation and information sharing that they support, have led to a number of enforcement successes—just a few of which I would like to highlight here.

Trade secrets and the Insider Threat. In March 2011, a former computer programmer at Goldman Sachs & Co. was sentenced in Manhattan federal court to 97 months in prison for stealing valuable, proprietary computer code of Goldman Sachs. A jury previously found the defendant guilty of theft of trade secrets and interstate transportation of stolen property.

In February 2011, a former trader at Société Générale was sentenced in Manhattan to 36 months in prison for theft of trade secrets and interstate transportation of stolen property. In November 2010, a jury convicted the trader of stealing proprietary computer code used in the company's high frequency trading business and of interstate transportation of the stolen code.

Also in February 2011, a federal jury in Louisiana convicted a former research scientist of stealing trade secrets from Dow Chemical Company and selling them to companies in the People's Republic of China. According to the evidence presented in court, the defendant came to the United States from China for graduate work. He began working for Dow in 1965 and retired in 1992. Dow is a leading producer of the elastomeric polymer, chlorinated polyethylene (CPE). Dow's CPE is used in a number of applications worldwide, such as automotive and industrial hoses, electrical cable jackets and vinyl siding. The evidence at trial established that the defendant conspired with at least four current and former employees of Dow's facilities to misappropriate those trade secrets, in part by accessing Dow's computers, in an effort to develop and market CPE process design packages to various Chinese companies. The defendant traveled extensively throughout China to market the stolen information, and evidence introduced at trial showed that he paid current and former Dow employees for Dow's CPE-related material and information. The defendant is awaiting sentencing.

Global hacking and identity theft case. In August 2008, the Department, working closely with the Secret Service, announced one of the largest hacking and identity theft cases ever prosecuted, in which charges were brought by the USAOs in the District of Massachusetts, the Southern District of California, and the Eastern District of New York against 11 members of an international hacking ring responsible for the theft and sale of more than 40 million credit and debit card numbers obtained from various retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave &

Buster's, and DSW. The various defendants—who were from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus—included one of the top traffickers in stolen account information in the world, Maksym Yastremski, and one of the world's top hackers, Albert Gonzalez. Gonzalez pleaded guilty and was sentenced to 20 years in prison. Yastremski was convicted on related charges in Turkey and was later sentenced to 30 years in prison.

Gonzalez and two unnamed hackers believed to be residing in Russia were also indicted for conspiring to hack into computer networks supporting major American retail and financial organizations and stealing data relating to more than 130 million credit and debit cards. Among the corporate victims were Heartland Payment Systems, 7-Eleven Inc., and Hannaford Brothers Co. Inc. Mr. Gonzalez pleaded guilty to the charges and received a sentence of over 20 years in prison to run concurrently with his other sentence.

Sophisticated ATM fraud hacking ring. In November 2009, the Department announced the indictment in the Northern District of Georgia of a sophisticated international hacking ring that executed a $9 million fraud scheme that involved five defendants from Estonia, one from Russia, and one from Moldova. The indictment charged various defendants with hacking into a computer network operated by the credit card processing company RBS WorldPay and using sophisticated techniques to compromise the data encryption used by RBS WorldPay to protect customer data on payroll debit cards. Once the defendants had compromised the encryption on the card processing system, the hacking ring allegedly provided a network of "cashers" with 44 counterfeit payroll debit cards. The cashers used these cards to withdraw over $9 million from more than 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. Remarkably, the $9 million loss occurred within a span of less than 12 hours. The five Estonian defendants have been arrested and charged in Estonia. One of these defendants was extradited to the United States in August 2010. Through this investigation, the FBI uncovered a previously undetected hacking technique that compromised the bank's encryption system. This information was disseminated throughout the banking sector to prevent further losses.

International Online Tax Fraud Scheme. In January 2011, a Belarusian national residing in Massachusetts pled guilty to crimes stemming from his participation in an international online scheme to steal income tax refunds from U.S. taxpayers around the country. From 2006 through 2007, the defendant's co-conspirators lured victims by operating "phishing" websites that falsely claimed to be authorized by the IRS to offer lower-income taxpayers free online tax return preparation and electronic tax return filing services. After taxpayers uploaded their tax information, co-conspirators in Belarus collected the data and altered the returns to increase the refund amounts and to direct these refunds to be deposited into U.S. bank accounts controlled by the defendant. They then caused the fraudulently altered returns to be e-filed with the IRS. The conspiracy ultimately caused the U.S. Treasury and various state treasury departments to deposit more than $200,000 in stolen refunds into bank accounts controlled by the defendant.

Large-scale spam. In December 2010, a Russian citizen was charged with violating the CAN-SPAM Act. The indictment alleged that the defendant knowingly and materially falsified header information in billions of spam emails on behalf of individuals who were selling counterfeit Rolexes, non-FDA approved herbal remedies, and counterfeit prescription medications. In payment, the defendant received hundreds of thousands of dollars. The defendant is alleged to have initiated the sending of these messages by use of his botnet, dubbed the "Mega-D" botnet. This botnet compromised the security of tens of thousands of computers in the United States and around the world. The Mega-D botnet was capable of sending ten billion spam email messages a day, all with false header information.

Romanian Fraud Rings. In April 2010, Romanian police arrested 70 suspects who allegedly were involved in eBay scams and other cybercrimes since 2006. These arrests were the result of an international investigation dubbed Operation Valley of the Kings – a joint operation among the FBI, the Secret Service, and the Romanian Directorate for Investigating Organised Crime and Terrorism, involving hundreds of law enforcement agents in multiple cities and more than 100 search warrants. The arrested individuals allegedly used phishing attacks to get the login credentials of eBay account holders and then used the accounts to auction nonexistent goods. Police estimate that victims suffered approximately $1 million in losses after sending money for winning "auctions" but receiving no goods. Approximately 800 victims have been identified, and it is believed that the perpetrators operated in Austria, Canada, Denmark, France, Germany, Italy, New Zealand, Spain, Sweden, Switzerland, and the United States.

* * *

These cases illustrate the broad scope of the Department's efforts to pursue cyber criminals. While the Department is proud of these cases and all of our efforts to tackle the growing and evolving cybersecurity problem, we recognize that there is much more to be done, and we will continue to work with our law enforcement and private sector partners to meet that challenge. Because of the global nature of the Internet and the related crimes it can facilitate, continued close coordination and cooperation with foreign law enforcement is critical to our collective success. Because our prosecutors understand the severe damage that computer crimes can have upon a victim, we continue to pursue appropriate cases, both large and small.

The Department of Justice stands ready to work with the Committee as it examines these important issues. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.